INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed



www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

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

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

Copyright © International Journal for Legal Research & Analysis. All rights reserved.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

FROM NARCO-ANALYSIS TO DIGITAL FORENSICS: EVIDENTIARY CHALLENGES IN INDIAN COURTS

AUTHORED BY – AJAY & DR. HARSHITA THALAWAL

Abstract

Indian evidence law has moved from distrusting mind-based scientific techniques to depending on machine-based ones, but the core problem has not changed: courts must decide whether a scientific output is admissible, reliable and obtained lawfully. This paper traces that arc from narco-analysis, polygraph and Brain Electrical Oscillation Signature (BEOS) profiling, which the Supreme Court confined in Selvi v. State of Karnataka (2010) and again in Amlesh Kumar v. State of Bihar (2025), to the digital-evidence regime of Section 65B of the Indian Evidence Act, 1872 and its successor, Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 (BSA), in force from 1 July 2024.

Using doctrinal analysis of statutes and leading judgments, supported by National Crime Records Bureau (NCRB) data, the paper argues three points. First, the constitutional guarantees in Articles 20(3) and 21 settled the narco-analysis question, but not the parallel question of compelled access to devices and passwords. Second, the certificate model under Section 63(4), now carrying a mandatory hash value and upheld in Pune Bar Association v. Union of India (2026), answers admissibility but not reliability. Third, forensic capacity, chain-of-custody discipline and synthetic media (deepfakes) are now the binding constraints, not statutory text. The paper closes with a reform agenda: a reliability standard for scientific evidence, accredited digital-forensic capacity at district level, and statutory rules on compelled decryption.

Keywords: *narco-analysis; Article 20(3); scientific evidence; electronic evidence; Section 65B; Section 63 BSA; hash value; chain of custody; digital forensics; deepfakes; right to privacy.*

ISSN: 2582-6433

1. Introduction

Indian criminal courts now meet scientific evidence in two very different forms: techniques that try to read the suspect's mind, and techniques that read the suspect's devices. The first was largely closed off by constitutional adjudication in 2010. The second has become the dominant evidentiary form, with registered cybercrime rising from 27,248 cases in 2018 to 86,420 in 2023.[1]

The three new criminal codes, in force since 1 July 2024,[2] were drafted to make Indian investigation more scientific and less confession-driven. Yet each technological advance repeats an old pattern: the law first asks *is this admissible?*, then later realises the harder question is *can this be trusted, and was it obtained fairly?*

1.1 Statement of the research problem

Indian evidence law regulates scientific evidence through *form* (consent under *Selvi*, certificates under Section 63 BSA) rather than through an explicit *reliability* standard. This leaves courts without a structured test for evaluating the scientific validity of forensic outputs, and leaves investigators without clear limits on compelled access to digital data.

1.2 Research objectives

1. To trace the doctrinal evolution from narco-analysis to digital forensic evidence in Indian courts.
2. To analyse how Articles 20(3) and 21 shape the admissibility of both mind-based and machine-based evidence.
3. To evaluate the Section 65B / Section 63 BSA certificate regime against the problems of authenticity, integrity and synthetic media.
4. To assess institutional capacity, mainly forensic laboratories, as a determinant of evidentiary quality.
5. To propose a reform framework drawing on comparative practice in the United States and United Kingdom.

[1] National Crime Records Bureau, *Crime in India 2023* (Ministry of Home Affairs, Government of India, New Delhi, 2025); "Crimes Against STs, Cybercrimes Surged in 2023: NCRB Report" *The Wire*, *available at*: https://m.thewire.in/article/society/crimes-against-sts-cybercrimes-surged-in-2023-ncrb-report (last visited on November 12, 2026).

[2] The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023); The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023); The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), all in force from July 1, 2024.

ISSN: 2582-6433

1.3 Research questions

- **RQ1.** Did *Selvi* (2010) and *Amlesh Kumar* (2025) settle the place of narco-analysis in Indian trials, and on what reasoning?
- **RQ2.** Does the Section 63 BSA certificate, now with a mandatory hash value, ensure the *reliability* of digital evidence, or only its *admissibility*?
- **RQ3.** Does the *Selvi* reasoning on testimonial compulsion extend to compelled disclosure of passwords and biometric unlocking?
- **RQ4.** What institutional and procedural reforms would close the gap between the law on paper and forensic practice?

1.4 Hypothesis

H1: Indian law has shifted the risk in scientific evidence from **coercion of the accused** (narco-analysis) to **unreliability of the record** (digital evidence), but its safeguards remain procedural rather than scientific. Courts therefore admit digital evidence that satisfies certification formalities without a structured inquiry into its forensic validity.

1.5 Research methodology

The study is **doctrinal and analytical**, with a descriptive-empirical component.

Element	Approach
Primary sources	Constitution of India; Indian Evidence Act, 1872; Bharatiya Sakshya Adhiniyam, 2023; Bharatiya Nagarik Suraksha Sanhita, 2023; IT Act, 2000; Supreme Court and High Court judgments
Secondary sources	Law reports, commission reports, journal articles, law-firm and legal-news analysis
Empirical data	NCRB *Crime in India* series (2018–2023); parliamentary answers and state forensic-laboratory reports
Comparative method	Functional comparison with US (*Frye*, *Daubert*, FRE 702) and UK (PACE 1984, Criminal Practice Directions)
Limitations	NCRB data counts FIRs, not complaints; latest published year is 2023; no access to unreported trial-court records

1.6 Scope and chapter scheme

The paper covers criminal proceedings, with brief reference to civil use of electronic records. Section 2 sets the conceptual framework. Section 3 examines narco-analysis and allied

ISSN: 2582-6433

techniques. Sections 4 and 5 examine the electronic-evidence regime and its practical challenges. Section 6 offers a comparative view, and Sections 7 and 8 present findings and recommendations.

2. Conceptual Framework: Scientific Evidence and the Indian Gatekeeping Model

Indian courts test scientific evidence through three gates, but only the first two are written into statute. The third, scientific reliability, is left to judicial discretion under the expert-opinion provision.

2.1 Three questions every scientific exhibit must answer

1. **Legality of collection.** Was the evidence obtained without violating Articles 20(3) and 21, and in line with procedure under the BNSS (for example, Section 105 videography of search and seizure)?
2. **Admissibility.** Does it satisfy the statutory route, such as Section 63 BSA for electronic records, or Section 39 BSA for expert opinion?
3. **Reliability and weight.** Is the underlying technique valid, was it correctly applied, and is the result free of tampering?

Indian law has historically been strong on the first gate and formal on the second. It is thin on the third: there is no codified validity test of the *Daubert* type. Courts assess expert opinion as advisory, not binding, and weigh it with the rest of the record.

2.2 Admissibility is not reliability

A recurring confusion in Indian practice is to treat a valid certificate as proof that a record is genuine. Commentators have pointed out that compliance with Section 63 makes a record *admissible* but does not establish its authenticity, integrity or weight.[3] The paper uses this distinction as its main analytical lens.

[3] "Section 63, Bharatiya Sakshya Adhiniyam, 2023: Admissibility and Reliability of Electronic Records" *TaxGuru*, *available at*: https://taxguru.in/?p=1072828 (last visited on November 12, 2026).

ISSN: 2582-6433

2.3 The two eras compared

Dimension	Era I: mind-based techniques	Era II: machine-based techniques
Examples	Narco-analysis, polygraph, BEAP / BEOS (brain mapping)	Mobile and computer forensics, CCTV, call-detail records, cloud data, chat exports
Source of evidence	The suspect's mind and physiology	Devices, networks and service providers
Core legal risk	Testimonial compulsion; mental privacy	Tampering, broken chain of custody, mass data intrusion
Governing constitutional rule	Article 20(3) and Article 21 (*Selvi*, 2010)	Article 21 privacy (*Puttaswamy*, 2017); Article 20(3) unsettled for passwords
Statutory gate	None specific; consent and Section 27 discovery	Section 65B IEA, now Section 63 BSA with hash-value certificate
Scientific status	Contested; low validity for truth-detection	High validity in principle; depends on process and examiner
Judicial posture	Restrictive	Permissive on admission, cautious on weight

2.4 Theoretical lens

The analysis draws on two ideas. The **due-process model** of criminal justice (Herbert Packer)[4] explains why Indian courts protected the accused against mind-reading techniques. The **forensic-validity** literature, including the 2009 US National Research Council report and the 2016 PCAST report,[5] explains why procedural safeguards alone cannot guarantee reliable forensic output.

[4] Herbert L. Packer, *The Limits of the Criminal Sanction* (Stanford University Press, Stanford, 1968).
[5] National Research Council, *Strengthening Forensic Science in the United States: A Path Forward* (National Academies Press, Washington DC, 2009); President's Council of Advisors on Science and Technology, *Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods* (Executive Office of the President, Washington DC, 2016).

ISSN: 2582-6433

2.5 Doctrinal timeline

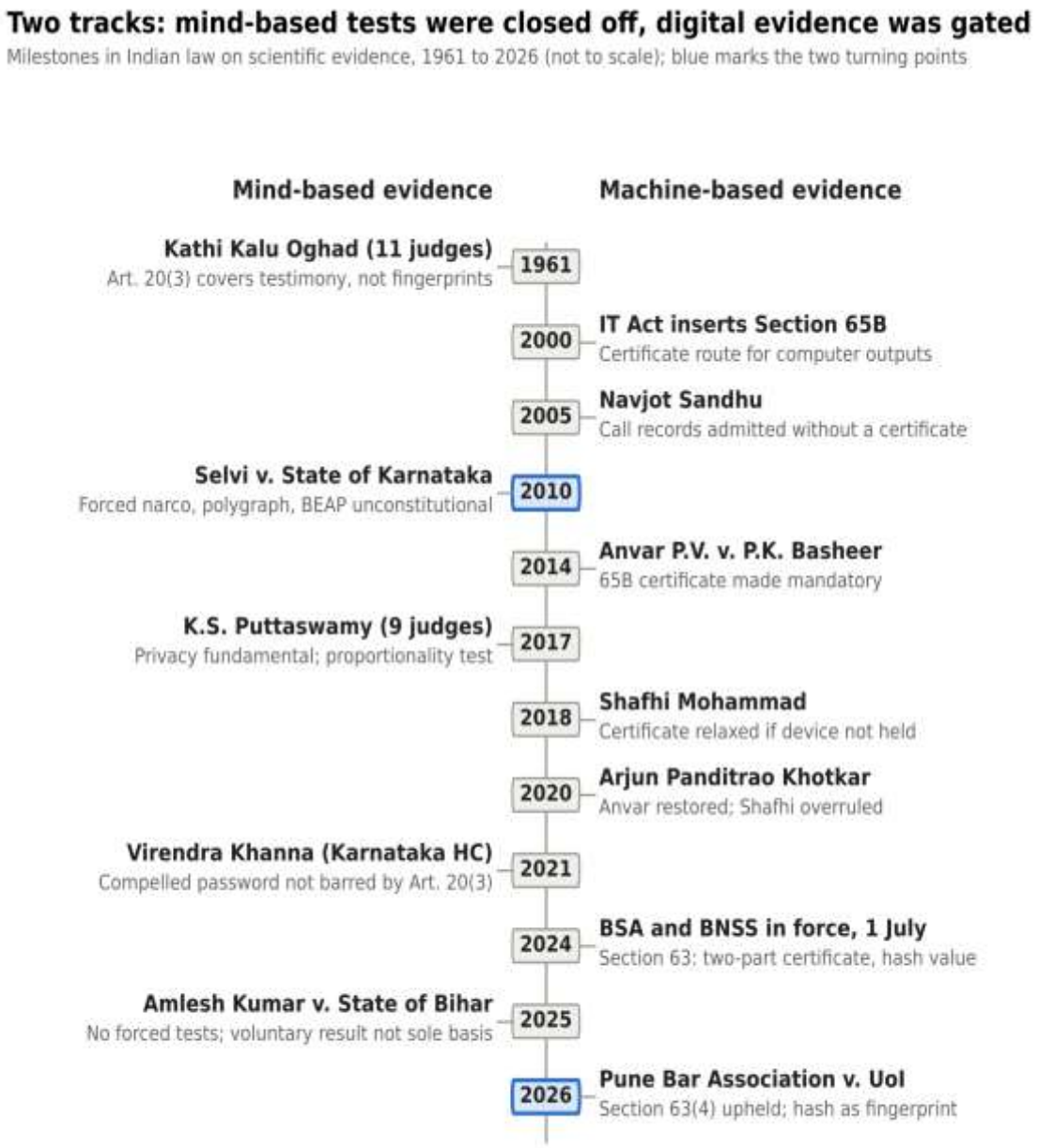


Figure 1: Doctrinal timeline of scientific evidence in Indian law, 1961–2026

The left track closed in 2010 and was reaffirmed in 2025; the right track swung between strict and relaxed certificate rules before settling on a hash-based certificate. *Virendra Khanna* (2021) is where the two tracks meet: a device password is machine access, but it sits in the mind.

ISSN: 2582-6433

3. Narco-Analysis and Deception-Detection Techniques

The Supreme Court has held, twice and unanimously, that no person can be subjected to narco-analysis, polygraph or brain-mapping without consent, and that even a voluntary test cannot by itself sustain a conviction.

3.1 The techniques and their scientific standing

- **Narco-analysis** involves intravenous administration of a barbiturate, typically sodium pentothal, to induce a semi-conscious state in which inhibition is lowered. Its premise, that a drugged subject cannot lie, is not supported by evidence: subjects may fantasise, become suggestible or repeat what interrogators imply.
- **Polygraph** records physiological responses (blood pressure, respiration, skin conductance) to questions. It measures arousal, not deception, and error rates vary widely with examiner skill and question format.
- **BEAP / BEOS** (Brain Electrical Activation Profile, Brain Electrical Oscillation Signature) records electrical activity when a subject is shown crime-related stimuli. It infers *experiential knowledge*, but peer-reviewed validation is limited.

All three share one feature: they try to extract information that exists only in the subject's mind. That is why Article 20(3) became the decisive frame.

3.2 Pre-*Selvi* position

In *State of Bombay v. Kathi Kalu Oghad* (1961), an eleven-judge bench[6] held that Article 20(3) protects against compelled *testimony*, meaning the imparting of personal knowledge, but not against compelled production of physical evidence such as fingerprints, handwriting or specimen signatures. Through the 2000s, investigating agencies used narco-analysis in high-profile cases, and several High Courts permitted it on the reasoning that the test results were not themselves statements.

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

A three-judge bench led by Chief Justice K.G. Balakrishnan held:[7]

1. Compulsory administration of narco-analysis, polygraph and BEAP violates **Article 20(3)**, because the results are testimonial: they convey personal knowledge, even when the subject does not speak voluntarily.

[6] *State of Bombay v. Kathi Kalu Oghad*, AIR 1961 SC 1808.
[7] *Selvi v. State of Karnataka*, (2010) 7 SCC 263.

ISSN: 2582-6433

2. Such compulsion also violates **Article 21**, as an unjustified intrusion into mental privacy and a form of cruel, inhuman or degrading treatment.
3. The tests may be conducted only with **informed consent**, recorded before a Judicial Magistrate, with access to a lawyer, and following the National Human Rights Commission's 2000 guidelines on polygraph tests.[8]
4. Even voluntary test results are **not admissible as evidence** in themselves. Only material later discovered with the help of voluntarily given information may be admitted under Section 27 of the Evidence Act (now Section 23(2) proviso, BSA).

3.4 *Amlesh Kumar v. State of Bihar*, 2025 INSC 810

Fifteen years later, the Patna High Court, while hearing a bail matter, recorded a police officer's proposal to conduct narco-analysis on all accused and witnesses. On 9 June 2025, a bench of Justices Sanjay Karol and Prasanna B. Varale set this aside[9] as being in direct conflict with *Selvi*. The Court added three clarifications:

- A bail hearing is not the stage to order intrusive investigative techniques.
- A voluntary test report, even with safeguards, **cannot be the sole basis of conviction**.
- The accused has **no indefeasible right** to demand a narco test; the court may permit a voluntary test at the defence-evidence stage, given its suspect scientific nature. The bench disapproved the Rajasthan High Court's contrary view in *Sunil Bhatt*.

3.5 Position under the new codes

The BNSS and BSA contain no provision authorising narco-analysis, polygraph or brain-mapping. Section 349 BNSS widens the magistrate's power to order specimen signatures, handwriting, finger impressions and voice samples, extending the reasoning of *Ritesh Sinha v. State of Uttar Pradesh* (2019)[10] on voice samples. Those are *physical* evidence under *Kathi Kalu Oghad*, not testimonial, and so fall outside the *Selvi* bar.

3.6 Assessment

The narco-analysis question is constitutionally settled. What remains unsettled is its logic: the

[8] National Human Rights Commission, *Guidelines Relating to Administration of Polygraph Test (Lie Detector Test) on an Accused* (2000); *Selvi*, *supra* note 7.
[9] *Amlesh Kumar v. State of Bihar*, 2025 INSC 810 (decided on June 9, 2025), *available at*: https://api.sci.gov.in/supremecourt/2024/9701/9701_2024_4_1501_62184_Judgement_09-Jun-2025.pdf (last visited on November 12, 2026).
[10] *Ritesh Sinha v. State of Uttar Pradesh*, (2019) 8 SCC 1; The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023), s. 349.

ISSN: 2582-6433

line Selvi drew between mental knowledge (protected) and physical evidence (unprotected) now has to be applied to smartphones, which store a person's thoughts outside the body. Section 5.5 returns to this question.

4. The Transition to Digital Evidence: From Section 65B to Section 63 BSA

After two decades of conflicting rulings, the law now holds that a certificate is mandatory for secondary electronic evidence, and since 1 July 2024 that certificate must carry a hash value and an expert's part.

4.1 Statutory origin

The Information Technology Act, 2000 inserted Sections 65A and 65B into the Indian Evidence Act. Section 65B(2) set four conditions for a computer output to be admissible without the original: regular use of the computer, regular feeding of the information, proper operation, and derivation from information fed in the ordinary course. Section 65B(4) required a certificate signed by a responsible official.[11]

4.2 The judicial see-saw, 2005–2020

Year	Case	Holding	Effect
2005	*State (NCT of Delhi) v. Navjot Sandhu* (Parliament attack)[12]	Call records admissible through oral evidence and Sections 63 and 65 IEA, even without a 65B certificate	Certificate seen as optional
2014	*Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473	Section 65B is a complete code; certificate mandatory for secondary electronic evidence; *Navjot Sandhu* overruled on this point	Certificate made mandatory
2018	*Shafhi Mohammad v. State of H.P.*, (2018) 2 SCC 801	Certificate can be dispensed with where the party does not possess the device	Requirement relaxed
2020	*Arjun Panditrao Khotkar v. Kailash*	*Anvar* reaffirmed; *Shafhi* overruled; certificate not needed when original device is	Certificate mandatory,

[11] The Indian Evidence Act, 1872 (Act 1 of 1872), ss. 65A–65B, inserted by The Information Technology Act, 2000 (Act 21 of 2000).
[12] *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 SCC 600; *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473; *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801; *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.

ISSN: 2582-6433

Year	Case	Holding	Effect
	Gorantyal, (2020) 7 SCC 1	produced; may be filed late, subject to fairness to the accused	flexible on timing

4.3 What Section 63 BSA changed

Section 63 BSA, effective from 1 July 2024, carries forward the four conditions and the certificate model, but adds two safeguards: a two-part certificate and a mandatory hash value.[13] It also expressly covers communication devices and semiconductor memory, not just computers.

Feature	Section 65B IEA, 1872	Section 63 BSA, 2023
Devices covered	Computer	Computer and communication device, including semiconductor memory and smartphones
Certificate	One certificate by a person in a responsible official position	Schedule certificate: **Part A** by the party producing the record; **Part B** by an expert
Integrity marker	None prescribed	**Hash value** of the record (for example SHA-256) must be disclosed
Primary evidence	Original device	Expanded by Section 57 BSA explanations: each stored copy in the ordinary course can be primary evidence
Expert opinion	Section 45A IEA (Examiner of Electronic Evidence)	Section 39(2) BSA (Examiner notified under Section 79A IT Act)

4.4 *Pune Bar Association v. Union of India* (2026)

On 22 May 2026, a three-judge bench (Chief Justice Surya Kant, Justices Joymalya Bagchi and Vipul M. Pancholi) rejected a challenge to Section 63(4) and the Schedule.[14] The petitioner had argued that the hash-value and expert requirements placed an excessive burden on ordinary litigants.[15] The key holdings:

- Electronic records are vulnerable to alteration, and the risk has grown with AI and

[13] The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), s. 63(4) and Schedule; "Admissibility of Electronic Evidence under Section 63 BSA" *LawSikho, available at*: https://lawsikho.com/blog/?p=7126 (last visited on November 12, 2026).
[14] *Pune Bar Association v. Union of India*, 2026 SCC OnLine SC 1297 (decided on May 22, 2026).
[15] Ritu, "Hash value is an electronic fingerprint; Section 63(4) BSA certificate requirement is valid: Supreme Court" *SCC Times*, July 8, 2026, *available at*: https://www.scconline.com/blog/post/2026/07/08/sc-upholds-admissibility-of-electronic-evidence-under-section-63-4-bsa/ (last visited on November 12, 2026).

ISSN: 2582-6433

deepfake tools; the Court described the hash value as an electronic fingerprint for verifying data.

- The Part B expert certification adds a further layer of authenticity, and the provision has a rational nexus with its object, so it is not manifestly arbitrary.
- Reading Sections 39(1) and 39(2) BSA together, a person with proven skill in computer science and cyber forensics, not only a Section 79A-notified examiner, may sign Part B if the court is satisfied on unimpeachable material. The Madras High Court's narrower view is not binding precedent, and the question is left open for a suitable case.

4.5 Assessment

The law has moved from **no integrity check** (2005) to a **formal integrity check** (2026). The hash value is a genuine scientific safeguard, but it proves only that the copy matches the source *at the time of hashing*. It says nothing about whether the source was authentic, or whether it was altered before it was hashed. That gap is the subject of Section 5.

5. Digital Forensics in Practice: The Real Evidentiary Challenges

The binding constraints on digital evidence in India are now practical rather than textual: volume, forensic capacity, chain-of-custody discipline, synthetic media and the unresolved law on compelled decryption.

5.1 Scale of the problem

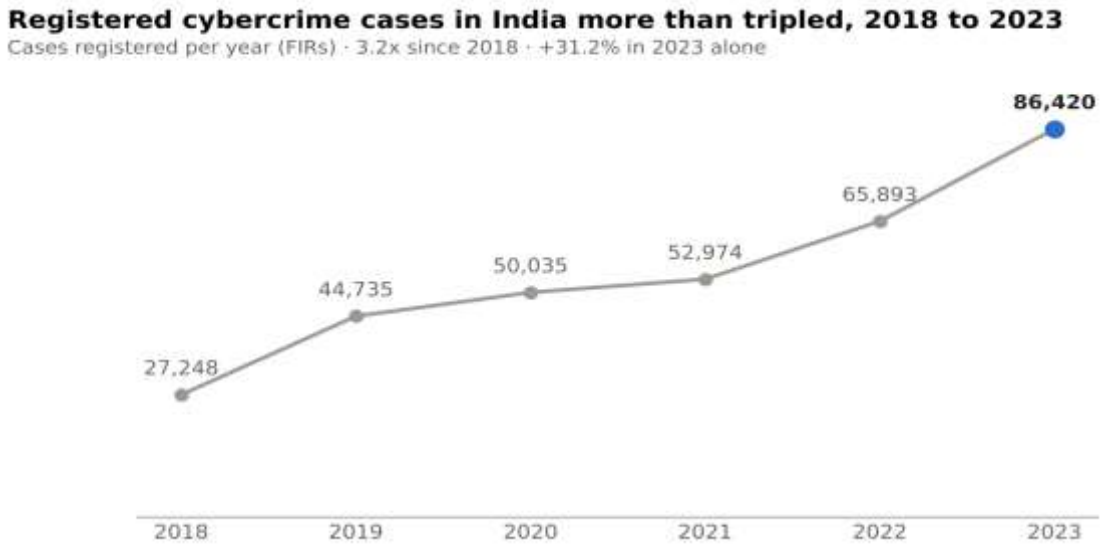


Figure 2: Registered cybercrime cases in India, 2018–2023 (Source: NCRB, Crime in India)

Cybercrime registrations rose 31.2% in 2023 alone, and fraud accounted for 68.9% of cases

ISSN: 2582-6433

(59,526).[16] These are FIR counts. RTI data cited for Mumbai suggests only about 2% of complaints on the National Cyber Crime Portal became FIRs,[17] so the evidentiary load is far larger than the chart shows. Digital evidence is also now routine in conventional crimes: CCTV, call-detail records and chat messages feature in murder, dowry and narcotics trials.

5.2 Chain of custody and the moment of seizure

The hash value under Section 63(4) protects a record only *after* it is hashed. Most disputes arise earlier: at seizure, before imaging, or when an officer browses a seized phone without a write-blocker. The BNSS responds in two ways:

- **Section 105 BNSS** requires audio-video recording of searches and seizures, including preparation of the seizure list.
- **Section 176(3) BNSS** requires a forensic expert to visit the scene, and videography of evidence collection, for offences punishable with seven years or more. Each State has five years from commencement to notify the date from which the duty applies.[18]

Neither provision states a consequence for non-compliance. Commentators expect that failure to video-record will reduce evidentiary weight rather than invalidate the seizure.[19] Videography also creates *more* electronic records, each of which must itself satisfy Section 63.

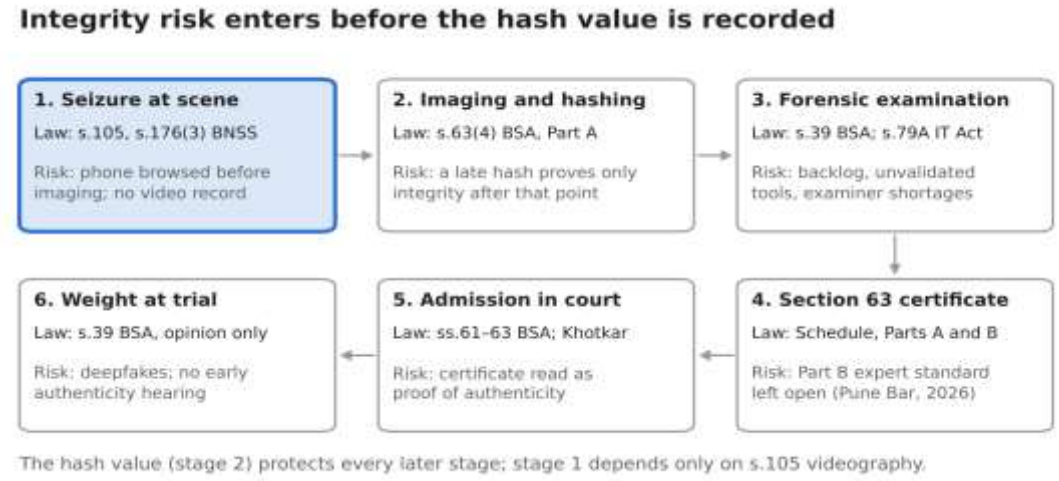


Figure 3: The life of a digital exhibit, from seizure to judgment

[16] "Crime in India 2023 – NCRB Report Highlights Surge in Cybercrime in India" *Vajiram & Ravi*, *available at*: https://vajiramandravi.com/current-affairs/?p=65786 (last visited on November 12, 2026).
[17] "Screens of Silence: What NCRB Data Misses about Cybercrime in India" *Sabrang India*, *available at*: https://sabrangindia.in/screens-of-silence-what-ncrb-data-misses-about-cybercrime-in-india/ (last visited on November 12, 2026).
[18] The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023), ss. 105, 176(3); "Mandatory Forensic Investigation under Section 176(3) BNSS" *iPleaders*, *available at*: https://blog.ipleaders.in/?p=130128 (last visited on November 12, 2026).
[19] "Will Failure to Video-Record a Search Make Seizure Illegal? Expert Opinion on S. 105, 185 & 176(3) BNSS" *JurisHour*, *available at*: https://www.jurishour.in/?p=1442452 (last visited on November 12, 2026).

ISSN: 2582-6433

Only stage 1 sits outside the protection of the hash value, which is why seizure practice decides most authenticity disputes.

5.3 Forensic capacity

Capacity has grown but unevenly:

- The Ministry of Home Affairs has set up a National Cyber Forensic Laboratory at the Central Forensic Science Laboratory, Hyderabad.[20]
- Under the I4C-linked schemes, cyber forensic-cum-training labs have been funded in 33 States and UTs, over 550 mobile forensic vans operate in districts, and over 24,600 officials had been trained by 2025.[21] The same analysis reports staff shortages and high attrition of trained examiners.
- State variation is large. Delhi FSL reported cutting its pendency from about 27,000 to about 5,700 cases in roughly a year.[22] Haryana expanded its cyber forensic division from one to six reporting officers, with 24 more under recruitment, while the India Justice Report 2025 flagged high vacancies in West Bengal.

The Part B expert certificate under Section 63(4) depends directly on this capacity. *Pune Bar Association* eased the bottleneck by allowing non-notified experts, but left the standard for such experts undefined.

5.4 Synthetic media and the "deepfake defence"

Generative AI creates two opposite risks. Fabricated audio, video or chat records may be tendered as genuine. Conversely, genuine records may be attacked as fake, often called the *liar's dividend*. A Section 63 certificate does not resolve either risk, because a deepfake can be hashed and certified like any other file.[23] The BSA has no provision specific to synthetic media, and commentators note the absence of an accredited lab network for deepfake detection.

[20] Ministry of Home Affairs, Government of India, Rajya Sabha Unstarred Question No. 1520, answered on March 12, 2025, *available at*: https://rsdebate.nic.in/bitstream/123456789/757376/1/PQ_267_12032025_U1520_p330_p334.pdf (last visited on November 12, 2026).

[21] Khushhal Kaushik, "India's Cyber Forensics Push Since 2020: Building National Capacity for Digital Investigations" *Observer Research Foundation*, *available at*: https://www.orfonline.org/expert-speak/india-s-cyber-forensics-push-since-2020-building-national-capacity-for-digital-investigations (last visited on November 12, 2026).

[22] United News of India, report on pendency at the Forensic Science Laboratory, Delhi, November 4, 2026, *available at*: https://www.uniindia.com/national/forensic-del-rfsl-sood/236264 (last visited on November 12, 2026); see also "Haryana Races Towards Zero Forensic Backlog" *The Statesman*, *available at*: https://www.thestatesman.com/india/haryana-races-towards-zero-forensic-backlog-1503468784.html (last visited on November 12, 2026).

[23] "AI Deepfakes as Evidence: Why Section 63 Certification Does Not Prove Content Authenticity" *TaxGuru*, *available at*: https://taxguru.in/?p=1076060 (last visited on November 12, 2026).

ISSN: 2582-6433

5.5 Compelled decryption: the unfinished *Selvi* question

In *Virendra Khanna v. State of Karnataka* (2021), a single judge of the Karnataka High Court held that directing an accused to disclose a password or provide biometrics to unlock a device does not violate Article 20(3).[24] A Special CBI Court in Delhi later took the opposite view, holding the accused protected by Article 20(3) and the right to silence.[25] The Supreme Court has not decided the question.

The *Selvi* test suggests a distinction. A **biometric** unlock uses a physical characteristic, much like a fingerprint under *Kathi Kalu Oghad*. A **password** is held only in memory, and disclosing it conveys personal knowledge, which is closer to the testimony *Selvi* protected. Scholars have argued that both should be protected under Article 20(3).[26]

5.6 Privacy, over-seizure and proportionality

A modern phone holds years of private life. *K.S. Puttaswamy v. Union of India* (2017)[27] requires that any State intrusion into privacy satisfy legality, legitimate aim and proportionality. Indian law has no statutory rule limiting a device search to data relevant to the offence, no time limit on retention of extracted images, and no requirement of a judicial warrant for device examination after seizure.

5.7 Cross-border and cloud data

Email, messaging and cloud data are often held by foreign service providers. Section 94 BNSS lets courts and police summon electronic documents, but access to foreign-held content still depends on mutual legal assistance treaties or provider cooperation. Delays here often decide whether a certified record can be obtained at all.

6. Comparative Perspective: United States and United Kingdom

Both comparator systems separate admissibility from reliability more explicitly than India does, and both have dealt directly with compelled decryption.

[24] *Virendra Khanna v. State of Karnataka*, 2021 SCC OnLine Kar 5032 (decided on March 12, 2021).
[25] Report on order of the Special CBI Court, Delhi, on compelled disclosure of passwords, *TaxGuru*, *available at*: https://taxguru.in/corporate-law/accused-compelled-password-electronic-device-investigation-proceedings.html (last visited on November 12, 2026).
[26] XI(2) *NLIU Law Review* 145–158 (2022), *available at*: https://nliulawreview.nliu.ac.in/wp-content/uploads/2022/09/Vol-XI-Issue-II-145-158.pdf (last visited on November 12, 2026).
[27] *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

ISSN: 2582-6433

6.1 United States

- **Reliability gate.** *Frye v. United States* (1923)[28] admitted scientific evidence only if "generally accepted" in the relevant field. *Daubert v. Merrell Dow Pharmaceuticals* (1993)[29] made the trial judge a gatekeeper who weighs testability, peer review, known error rate, standards and general acceptance. Federal Rule of Evidence 702, amended in 2023, requires the proponent to show reliability on the balance of probabilities.
- **Polygraph.** Most federal and state courts exclude polygraph results; *United States v. Scheffer* (1998)[30] upheld a blanket military ban, citing lack of scientific consensus.
- **Digital authentication.** FRE 901 and the 2017 additions FRE 902(13)–(14) allow self-authentication of electronic records and copies verified by hash value, through a certificate of a qualified person.
- **Device privacy.** *Riley v. California* (2014)[31] requires a warrant to search a phone seized on arrest; *Carpenter v. United States* (2018)[32] requires a warrant for historical cell-site data.
- **Compelled decryption.** Courts are divided. The Fifth Amendment usually protects compelled disclosure of a passcode, while biometric unlocking is often treated as non-testimonial; the "foregone conclusion" doctrine is applied inconsistently.

6.2 United Kingdom

- **Exclusion discretion.** Section 78 of the Police and Criminal Evidence Act 1984 (PACE) lets courts exclude evidence whose admission would harm the fairness of proceedings, including unlawfully obtained digital evidence.
- **Reliability of expert evidence.** Following the Law Commission's 2011 report,[33] Part 19 of the Criminal Procedure Rules and the Criminal Practice Directions require experts to disclose the basis and limits of their methods, and invite courts to test reliability.
- **Electronic records.** There is no special certificate rule; a presumption that computers were working properly operates, and has been heavily criticised after the Post Office

[28] *Frye v. United States*, 293 F. 1013 (D.C. Cir. 1923).
[29] *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993); Federal Rules of Evidence (United States), r. 702.
[30] *United States v. Scheffer*, 523 U.S. 303 (1998).
[31] *Riley v. California*, 573 U.S. 373 (2014).
[32] *Carpenter v. United States*, 585 U.S. 296 (2018).
[33] Law Commission of England and Wales, *Expert Evidence in Criminal Proceedings in England and Wales* (Law Com No. 325, 2011).

ISSN: 2582-6433

Horizon miscarriages of justice.[34]

- **Compelled decryption.** Section 49 of the Regulation of Investigatory Powers Act 2000 permits a notice requiring disclosure of a key or password, with refusal an offence under Section 53 (up to two years, or five in national security and child indecency cases).
- **Forensic standards.** Since 2023 the Forensic Science Regulator Act 2021 has made compliance with the Regulator's Code of Practice a statutory requirement, including for digital forensics.

6.3 Comparative matrix

Issue	India	United States	United Kingdom
Narco / polygraph	Barred without consent; voluntary result not sole basis (*Selvi*, *Amlesh Kumar*)	Polygraph generally excluded; narco not used	Not used as evidence
Reliability test for science	None codified; Section 39 BSA expert opinion is advisory	*Daubert* / FRE 702 gatekeeping	CrimPR Part 19; PACE s.78
Digital admissibility	Mandatory Section 63(4) certificate with hash value	Authentication under FRE 901 / 902(13)–(14)	Common-law presumption of proper working
Forensic lab regulation	Section 79A notified examiners; no statutory regulator	Accreditation largely voluntary; state-level variation	Statutory Forensic Science Regulator
Compelled password	Unsettled (*Virendra Khanna* vs. contrary trial-court view)	Usually protected by Fifth Amendment	Statutory duty under RIPA s.49
Warrant for phone search	Not required beyond seizure powers	Required (*Riley*)	Statutory powers under PACE and the Criminal Justice and Police Act 2001

[34] *Bates v. Post Office Ltd. (No. 6)*, [2019] EWHC 3408 (QB); *Hamilton v. Post Office Ltd.*, [2021] EWCA Crim 577.

ISSN: 2582-6433

6.4 Lessons for India

The US experience shows the value of an explicit reliability test. The UK experience shows two warnings: a presumption of computer reliability can produce miscarriages of justice (Horizon), and a statutory regulator can raise forensic standards. India's certificate model is stricter than both at the admissibility stage, but has no equivalent of their reliability or regulatory machinery.

7. Findings and Analysis

The hypothesis is broadly supported: Indian law has moved the main evidentiary risk from coercion of the accused to unreliability of the record, while its safeguards remain mostly procedural.

Research question	Finding	Status
RQ1. Is narco-analysis settled?	Yes. *Selvi* (2010) and *Amlesh Kumar* (2025) bar involuntary tests under Articles 20(3) and 21; voluntary results are not substantive evidence and cannot alone convict.	Supported
RQ2. Does the Section 63 certificate secure reliability?	Only partly. The hash value secures integrity *after* acquisition; it cannot prove authenticity at source or detect synthetic content.	Supported
RQ3. Does *Selvi* extend to passwords?	Unsettled. *Virendra Khanna* permits compulsion; a contrary Delhi trial-court view exists; the Supreme Court has not ruled. *Selvi*'s logic favours protecting passwords but not biometrics.	Open
RQ4. What closes the gap?	Capacity, standards and a reliability test, not further admissibility formalities (Section 8).	Supported

7.1 Key analytical findings

1. **Continuity of the core problem.** Narco-analysis and digital forensics both raise the same three questions: was the evidence lawfully obtained, is it admissible, and is it reliable? India answered the first question decisively for narco-analysis, but not yet for devices.[35]

[35] *Selvi*, *supra* note 7; *Amlesh Kumar*, *supra* note 9; *Virendra Khanna*, *supra* note 24.

ISSN: 2582-6433

2. **Formalism over validity.** The *Anvar–Khotkar–Pune Bar* line focuses on whether a certificate exists and who signs it. Trial courts rarely examine extraction tools, error rates or examiner competence.[36]
3. **Procedure without consequence.** Sections 105 and 176(3) BNSS require videography and forensic presence, but state no consequence for breach, and Section 176(3) depends on State notification.[37]
4. **Capacity is the real gate.** Part B certification, deepfake detection and timely reports all depend on forensic laboratories whose staffing and pendency vary widely across States.[38]
5. **Synthetic media changes the burden.** As forged content becomes cheap, the presumption that a recording shows a real event weakens. Courts will need an early, structured authenticity inquiry rather than leaving the question to cross-examination.[39]
6. **Privacy is under-regulated.** After *Puttaswamy*, the absence of rules on scope, warrants and retention for device searches is the largest constitutional gap in the digital-evidence regime.[40]

8. Recommendations and Conclusion

India should add a reliability layer and a capacity layer on top of its admissibility rules, and settle compelled decryption by statute rather than case-by-case.

8.1 Legal and doctrinal reforms

1. **Codify a reliability test for scientific evidence.** Amend Section 39 BSA, or issue Supreme Court guidelines, requiring courts to consider validation, known error rate, adherence to standards and examiner competence before relying on forensic opinion, adapted from *Daubert* and CrimPR Part 19.[41]
2. **Define the Part B expert.** Following *Pune Bar Association*, prescribe minimum qualifications and accreditation for non-notified experts who sign Part B certificates.[42]

[36] *Supra* notes 12 and 14.
[37] *Supra* notes 18 and 19.
[38] *Supra* notes 20, 21 and 22.
[39] *Supra* note 23; "Artificial Reality vs Judicial Truth: Deepfake Evidence in Indian Courts" *Jus Corpus*, *available at*: https://www.juscorpus.com/?p=76876 (last visited on November 12, 2026).
[40] *K.S. Puttaswamy*, *supra* note 27.
[41] *Daubert*, *supra* note 29; Law Commission of England and Wales, *supra* note 33; The Criminal Procedure Rules 2020 (UK), Part 19.
[42] *Pune Bar Association*, *supra* note 14; The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), s. 39.

ISSN: 2582-6433

3. **Legislate on compelled decryption.** Distinguish passwords (testimonial, protected) from biometrics (physical), require judicial authorisation for any compulsion, and limit use to data relevant to the offence.[43]
4. **Warrant and scope rules for device searches.** Require a magistrate's order specifying the data categories to be examined, with deletion of irrelevant personal data after a fixed period,[44] consistent with *Puttaswamy* proportionality.
5. **Synthetic-media protocol.** Allow a party to raise a prima facie deepfake objection at the admission stage, triggering forensic examination before trial; consider a specific offence for tendering AI-fabricated evidence.[45]
6. **Consequences for procedural breach.** Specify that unexplained non-compliance with Sections 105 and 176(3) BNSS shifts the burden to the prosecution to prove integrity of the evidence.[46]

8.2 Institutional reforms

- A statutory **Forensic Science Regulator**, on the UK model,[47] with mandatory ISO/IEC 17025 accreditation for labs issuing digital-evidence reports.
- **District-level cyber forensic units**, with time-bound notification of Section 176(3) by every State and published pendency data.
- Standardised **seizure-to-court SOPs**: write-blockers, immediate hashing at the scene, and logging on platforms such as e-Sakshya.
- **Judicial training** on hash values, extraction tools and deepfake indicators through the National and State Judicial Academies.
- Regular **NCRB reporting** on digital-evidence outcomes (cases where electronic evidence was rejected, and why), to give researchers an evidence base.

8.3 Suggestions for further research

- Empirical study of trial-court judgments on Section 63 objections after July 2024.
- Field study of Section 176(3) implementation across notified and non-notified States.
- Comparative study of deepfake-detection standards and their admissibility.

[43] The Regulation of Investigatory Powers Act 2000 (UK), ss. 49, 53; *Virendra Khanna*, *supra* note 24.
[44] *K.S. Puttaswamy*, *supra* note 27.
[45] The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023), ss. 227–229 (giving and fabricating false evidence); *supra* note 23.
[46] *Supra* note 18.
[47] The Forensic Science Regulator Act 2021 (UK).

ISSN: 2582-6433

8.4 Conclusion

The journey from narco-analysis to digital forensics is not a story of progress from bad science to good science. It is the same evidentiary question asked of a new source. With narco-analysis, the Supreme Court protected the mind of the accused and refused to trust a technique that could not prove its own reliability. With digital evidence, the courts have built a careful gate of certificates and hash values, but have not yet asked the scientific question with the same rigour, nor resolved how far the State may enter a phone that now functions as an extension of the mind. The task for the next decade is to carry *Selvi*'s constitutional seriousness and a genuine reliability standard into the digital era.

Bibliography

Statutes and rules

- *The Constitution of India, arts. 20(3), 21.*
- *The Indian Evidence Act, 1872 (Act 1 of 1872), ss. 27, 45A, 65A, 65B (repealed).*
- *The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023), ss. 227–229.*
- *The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023), ss. 94, 105, 176(3), 185, 349.*
- *The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), ss. 23, 39, 57, 61, 62, 63 and Schedule.*
- *The Information Technology Act, 2000 (Act 21 of 2000), s. 79A.*
- *Police and Criminal Evidence Act 1984 (UK), s. 78; Regulation of Investigatory Powers Act 2000 (UK), ss. 49, 53; Forensic Science Regulator Act 2021 (UK); Criminal Procedure Rules 2020 (UK), Part 19.*
- *Federal Rules of Evidence (US), rr. 702, 901, 902(13)–(14).*

Cases

- *Amlesh Kumar v. State of Bihar, 2025 INSC 810.*
- *Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.*
- *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.*
- *K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.*
- *Pune Bar Association v. Union of India, 2026 SCC OnLine SC 1297.*
- *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.*

ISSN: 2582-6433

- *State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600.*
- *State of Bombay v. Kathi Kalu Oghad, AIR 1961 SC 1808.*
- *Virendra Khanna v. State of Karnataka, 2021 SCC OnLine Kar 5032.*
- *Bates v. Post Office Ltd. (No. 6), [2019] EWHC 3408 (QB); Hamilton v. Post Office Ltd., [2021] EWCA Crim 577.*
- *Carpenter v. United States, 585 U.S. 296 (2018); Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993); Frye v. United States, 293 F. 1013 (D.C. Cir. 1923); Riley v. California, 573 U.S. 373 (2014); United States v. Scheffer, 523 U.S. 303 (1998).*

Books and reports

- *Herbert L. Packer, The Limits of the Criminal Sanction (Stanford University Press, Stanford, 1968).*
- *Law Commission of England and Wales, Expert Evidence in Criminal Proceedings in England and Wales (Law Com No. 325, 2011).*
- *National Crime Records Bureau, Crime in India 2022 and Crime in India 2023 (Ministry of Home Affairs, Government of India, New Delhi).*
- *National Human Rights Commission, Guidelines Relating to Administration of Polygraph Test (Lie Detector Test) on an Accused (2000).*
- *National Research Council, Strengthening Forensic Science in the United States: A Path Forward (National Academies Press, Washington DC, 2009).*
- *President's Council of Advisors on Science and Technology, Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods (Executive Office of the President, Washington DC, 2016).*

Articles and web sources

- *Khushhal Kaushik, "India's Cyber Forensics Push Since 2020: Building National Capacity for Digital Investigations" Observer Research Foundation.*
- *Ritu, "Hash value is an electronic fingerprint; Section 63(4) BSA certificate requirement is valid: Supreme Court" SCC Times (July 8, 2026).*
- *XI(2) NLIU Law Review 145–158 (2022).*
- *Web sources cited in the footnotes from TaxGuru, LawSikho, iPleaders, JurisHour, Vajiram & Ravi, Sabrang India, The Wire and Jus Corpus.*