Journal of Advances and Scholarly Researches in Allied Education
Vol. 20, Issue No. 3, July-2023, ISSN 2230-7540

DOI: https://doi.org/10.29070/d1843139

Check for updates

Strengthening Forensic Infrastructure in India: An Analytical Study of Institutional Deficits and Legal Challenges

Kanak Singh [1] *

1. Assistant Professor, Vidyasthali Law College (Affiliated by the Dr. B. R. Ambedkar Law University, Jaipur) Rajasthan, India
kanaksingh.92@gmail.com

Abstract: Forensic science has moved from the margins of criminal adjudication to its core, yet India's forensic ecosystem remains uneven in capacity, quality, and legal integration. This analytical article examines the institutional architecture of Indian forensics Central and State Forensic Science Laboratories (FSLs), specialized national institutions, accreditation regimes, and investigative interfaces and diagnoses structural bottlenecks such as funding asymmetry, skilled-personnel shortages, accreditation gaps, backlog accumulation, and fragile chain-of-custody practices. It maps the legal scaffolding under the Indian Evidence Act, the Code of Criminal Procedure (CrPC), the Information Technology Act, and recent measures like the Criminal Procedure (Identification) Act, 2022, while flagging unresolved privacy and proportionality concerns after the Puttaswamy privacy ruling. Through illustrative case-law on electronic evidence, scientific opinion, and consent in neuroscientific techniques, it evaluates how procedural rules and judicial standards shape the evidentiary value of forensic outputs. The article contrasts India's trajectory with international benchmarks the U.S. National Academies (2009) and PCAST (2016) critiques, the Daubert reliability gatekeeping approach, the U.K. Forensic Science Regulator's statutory powers, and ENFSI/ISO 17025 quality norms—to draw actionable lessons. It proposes a reform agenda centred on (i) a "quality-first" expansion model (mandatory accreditation, validated methods, blind proficiency testing), (ii) workforce pipelines via National Forensic Sciences University (NFSU)–State partnerships, (iii) digital-by-design evidence management integrated with ICJS/CCTNS, (iv) evidence-law updates to harmonize Sections 45, 45-A Evidence Act and Section 79A IT Act with Arjun Panditrao and Anvar P.V., and (v) rights-respecting bio-surveillance policies for DNA, biometric, and AI-enabled forensics. The article concludes that India's path to trustworthy, timely, and rights-compatible forensic science lies not in volume expansion alone but in rigorous standardization, sustained financing, and legal clarity that aligns scientific validity with constitutional values.

Keywords: Forensic science, Evidence law, DNA and biometrics, Electronic evidence, Chain of custody, Privacy, Criminal Procedure (Identification) Act, 2022, National Forensic Sciences University (NFSU), ICJS, Quality assurance, Judicial standards

X

INTRODUCTION

Across modern criminal justice systems, forensics supplies the bridge between investigative hypotheses and judicial proof. In India, that bridge is still under construction. The demand for timely, high-quality forensic outputs DNA profiling in sexual-offence cases, toxicology in suspicious deaths, ballistics in gun crimes, wildlife forensics under environmental statutes, and the full gamut of cyber/digital forensics has grown exponentially. Yet laboratory backlogs persist, accreditation remains partial, and evidentiary rules have not fully caught up with scientific practice or digital realities. Several national initiatives expansion of Central/State FSLs, specialized laboratories under the Directorate of Forensic Science Services (DFSS), the emergence of NFSU to build a workforce pipeline, the notification of "*Examiners of Electronic*

Evidence" under Section 79-A of the Information Technology Act, and digitization efforts like the Inter-operable Criminal Justice System (ICJS) signal intent. Still, the system faces entrenched deficits: uneven funding across States, weak procurement and maintenance cycles for sophisticated instrumentation, limited method validation, inconsistent documentation of chain of custody, insufficient court-facing scientific literacy, and frequent mismatch between investigatory timelines and laboratory throughput.

The legal architecture is likewise in transition. The Indian Evidence Act, 1872, built for a pre-DNA, pre-digital era, houses broad opinion-evidence provisions (Section 45) and, more recently, a statutory hook for electronic evidence (Section 45-A). The CrPC prescribes medical examination provisions (Sections 53, 53-A, 164-A) and recognizes expert-report admissibility (Section 293). The Information Technology Act enables the forensic authentication of electronic records via Section 65B of the Evidence Act and the Section 79-A examiner framework. The Criminal Procedure (Identification) Act, 2022, expands the universe of measurable biological/biometric parameters opening opportunities for robust identification but also intensifying privacy and proportionality concerns post-*Puttaswamy*. Indian courts have moved the needle on reliability in digital forensics (*Anvar P.V.*, *Arjun Panditrao*), but alignment between laboratory quality systems and legal admissibility remains incomplete.

This article offers (i) a historical and institutional mapping of Indian forensics, (ii) a granular diagnosis of deficits and legal challenges, (iii) a comparative lens on international best practices and pitfalls, and (iv) a reform blueprint that seeks not only faster laboratories but scientifically valid and rights-compatible forensic justice.

HISTORICAL BACKGROUND

Indian forensics evolved in waves. The early colonial era relied largely on medical jurisprudence and rudimentary chemical analysis. Post-Independence, forensic capabilities gradually diffused through State FSLs, supported by Central facilities (CFSLs) and specialized bodies such as the Central Forensic Science Laboratory network. The statutory bedrock the Indian Evidence Act, 1872 treated expert opinion as a species of relevant fact (Section 45), but left methodologies, validation thresholds, and quality control largely to professional practice.

From the 1970s onward, the CrPC structured interfaces between investigation and medical/forensic procedures, legitimizing medical examinations of accused and survivors (Sections 53, 53-A, 164-A) and permitting reliance on certain government expert reports without calling the expert (Section 293). With the IT Act, 2000, and the rapid digitization of commerce and communication, the evidentiary battlefield shifted: questions of hash integrity, metadata, provenance, and authenticity took centre stage. The legislature and the judiciary responded iteratively. Section 65B of the Evidence Act demanded a certificate for electronic records, Section 79-A IT Act later enabled the Union Government to notify Examiners of Electronic Evidence to standardize authenticity determinations. Judicially, *Anvar P.V. v. P.K. Basheer* (2014) re-anchored electronic evidence admissibility on Section 65B compliance, repudiating looser earlier readings, and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020) reaffirmed the certificate's centrality with limited pragmatic exceptions.

Parallelly, biosciences were transforming criminal investigation. DNA profiling became routine in sexual-

assault and homicide cases, but India's statutory DNA framework remained in flux. Earlier legislative attempts at human DNA profiling culminated in the DNA Technology (Use and Application) Regulation Bill, 2019, aimed at establishing data banks, laboratories, and regulatory oversight, yet, as of June 2023, a dedicated DNA statute had not been enacted. In this vacuum, DNA practice leaned on procedural provisions in CrPC, case-law, and laboratory SOPs, producing uneven consistency across jurisdictions.

Another inflection point arrived with neuroscientific and *"deception detection"* techniques. In *Selvi v. State of Karnataka* (2010), the Supreme Court proscribed compulsory narcoanalysis, polygraph, and BEAP tests, requiring informed consent and underscoring the primacy of mental privacy and bodily integrity. This jurisprudence foreshadowed the constitutional stakes that would later crystallize in *K.S. Puttaswamy v. Union of India* (2017), which recognized the fundamental right to privacy and demanded necessity and proportionality in State data practices principles directly relevant to biometric and DNA databases.

Institutionally, the Union created specialized national capacity and quality tools: the DFSS for coordinating Central Forensic Science Laboratories and issuing SOPs, NABL-driven laboratory accreditation to ISO/IEC 17025, and, in 2020, the establishment of NFSU to serve as a national talent and research hub. However, two systemic features continued to undermine reliability and timeliness. First, an enduring *"capacity-quality trap":* States expanded test menus (DNA, toxicology, wildlife forensics, cyber forensics) without matching investments in staff training, instrument maintenance, validation protocols, and quality assurance. Second, the *"throughput-justice mismatch*": statutory timelines and bail decisions increasingly hinge on forensic outputs, but laboratories struggle with surge loads, episodic funding, and uneven demand forecasting, spawning backlogs that can distort both investigation and adjudication.

The Criminal Procedure (Identification) Act, 2022, marks the latest structural shift. It broadens the definitional ambit of *"measurements"* to include biological samples and behavioural attributes, authorizes collection from a wider pool of persons, and lengthens retention periods seeking to modernize identification forensics. Yet, without harmonized rules on necessity thresholds, retention limits, expungement, and independent oversight, the Act risks friction with *Puttaswamy*'s proportionality doctrine. In short, India's historical arc reveals cumulative capability accretion, but also path-dependencies fragmented governance, uneven quality systems, and lagging legal harmonization that continue to shape today's forensic realities.

INSTITUTIONAL DEFICITS AND LEGAL CHALLENGES

1) **Capacity without uniform quality:** Many State FSLs operate with partial or no ISO/IEC 17025 accreditation across all disciplines. Where accreditation exists, method validation and measurement uncertainty are not consistently documented, blind proficiency testing is rare, and corrective-action learning loops remain under-institutionalized. This creates a courtroom vulnerability: without demonstrable reliability controls, forensic opinions risk being treated as conclusive by habit or discounted by suspicion, neither of which is scientifically appropriate.

2) **Backlogs and turnaround variability:** DNA, toxicology, and digital forensics often encounter the longest delays, driven by staff vacancies, high instrument downtime, and demand spikes in sexual-offence and narcotics cases. Turnaround time (TAT) variability amplifies pre-trial detention inequities and weakens deterrence, as evidence becomes stale and witnesses dislocate.

3) **Chain of custody and documentation fractures**: Paper-based transfer logs, inconsistent seals, and inadequate scene-to-lab digitization led to provenance disputes. Courts increasingly expect hash-based integrity for digital media and tamper-evident packaging with photographic logs for physical evidence. Absent robust documentation, the probative value of otherwise sound science can be undermined.

4) **Fragmented governance and procurement:** FSLs depend on State budgets, yet method standardization and strategic procurement (for HPLC-MS/MS, GC-MS, NGS sequencers, digital forensics suites) benefit from pooled purchasing and central technical guidance. Fragmentation leads to heterogeneous kits, variable maintenance contracts, and skills mismatch.

5) **Workforce pipeline constraints**: Forensic science demands cross-trained chemists, biologists, computer scientists, statisticians, and quality managers. Recruitment cycles are slow, career ladders are shallow, and court-facing training (report writing, testimony skills, Daubert-style reliability exposition) is limited. NFSU and select public universities have expanded seats, but alignment with State vacancy maps is imperfect.

6) **Electronic evidence admissibility friction**: After *Anvar P.V.* and *Arjun Panditrao*, Section 65-B certification is critical to admission of electronic records. Investigating officers often procure devices but lag in obtaining timely certificates from the "computer resource" owner, examiners under Section 79A are not uniformly leveraged, and standard operating procedures for imaging, hashing, and live-forensics collection vary. The mismatch between judicially required formalities and field practice produces exclusion risks.

7) **Bio-surveillance, privacy, and proportionality.** The Criminal Procedure (Identification) Act, 2022, widens collection and retention of biometric/biological data. In the *Puttaswamy* era, bulk retention without tailored necessity, purpose limitation, strong access controls, and independent oversight courts constitutional challenge. Lacking a dedicated DNA statute as of June 2023, governance relies on dispersed rules and internal SOPs, heightening legal uncertainty.

8) **Courtroom translation of science.** Judges and lawyers are asked to evaluate population genetics statistics (random match probability), error rates in toolmark and pattern disciplines, or confidence intervals in toxicology—areas that require scientific literacy and adversarial testing. Absent court-appointed neutral experts or structured tutorials, fact-finding can either over-credit or under-credit forensic conclusions.

9) **Interoperability and data standards.** ICJS and CCTNS promise end-to-end digitization—FIR to charge-sheet to evidence to judgment. But integrating laboratory information management systems (LIMS) with police and prosecution databases requires uniform schemas, API standards, audit logs, and privacy-by-design principles. Without these, evidence tracking and disclosure obligations remain brittle.

10) **Ethical governance and conflicts.** Where the same laboratory services both prosecution and defence only rarely, perceptions of partisanship arise, conversely, if laboratories are embedded within police hierarchies, independence concerns surface. Clear charters, publication of quality metrics, and transparent corrective-action summaries can bolster trust.

INTERNATIONAL PERSPECTIVES

Comparative experience clarifies both opportunities and cautionary tales. The 2009 report of the U.S. National Academies, *Strengthening Forensic Science in the United States: A Path Forward*, exposed deep methodological and quality-system gaps in several forensic disciplines, urging independence from law enforcement, mandatory accreditation, and research investments. The 2016 U.S. PCAST report sharpened the reliability lens, distinguishing feature-comparison methods with established validity (e.g., single-source, high-quality DNA) from those needing stronger empirical foundations (e.g., bite marks, certain pattern evidence). U.S. courts, under the *Daubert* standard, demand that judges act as gatekeepers assessing testability, peer review, known error rates, and general acceptance criteria that align with ISO/IEC 17025 quality constructs and should inspire Indian courtroom practice even though *Daubert* is not directly transplanted here.

In the U.K., chronic concerns over laboratory failures and uneven quality led to statutory powers for the Forensic Science Regulator in 2021, enabling enforcement of codes of practice and conduct. This model independent regulation with sanctioning capacity offers a template for India: DFSS/NABL could be complemented by a national regulator with powers to mandate accreditation, proficiency testing, and incident reporting across public and private providers.

European networks such as ENFSI have developed best-practice manuals and collaborative proficiency schemes, while GDPR foregrounds data-protection baselines of purpose limitation, data minimization, storage limitation, and accountability principles directly relevant to Indian discussions on DNA and biometric repositories. Australia and New Zealand's ANZPAA NIFS emphasizes national consistency, workforce development, and research translation, integrating laboratories and policing through standards and shared capability planning.

These comparators converge on a single insight: scaling forensics without embedding rigorous validation, accreditation, and independent oversight invites systemic error. Conversely, rights-respecting data governance can coexist with investigative efficacy when collection is specific, retention is bounded, access is audited, and oversight is real not merely notional.

CONCLUSION

India's forensic system sits at a critical juncture. Investment is rising, NFSU and DFSS have expanded training and guidance, ICJS/CCTNS can deliver digital chain-of-custody gains, and legal doctrine on electronic evidence is more coherent than a decade ago. Yet three fault lines remain: (i) quality assurance is not universal or uniformly deep, (ii) legal alignment on bio-surveillance and digital forensics still has gaps, and (iii) human capital and courtroom-translation capacity lag behind technological acquisition. The goal cannot be a mere increase in sample throughput. The north star is trustworthy forensics—methods validated, labs accredited, analysts competent and continuously proficiency-tested, documentation airtight, and rights protected. If pursued with discipline, such a system will shorten trial timelines, reduce wrongful convictions and acquittals alike, and enhance public confidence in the rule of law.

FUTURE SCOPE

1. **Legislative harmonization.** Update the Evidence Act to explicitly codify reliability criteria for

scientific evidence (error rates, validation, accreditation status), align Section 45/45-A with digital and bioscience realities, and clarify the status of laboratory reports across disciplines. Finalize a dedicated DNA framework with strict purpose limitation, retention ceilings, expungement rights, and independent oversight in line with *Puttaswamy*.

2. **Independent regulation.** Consider a statutory Forensic Science Regulator for India, empowered to mandate ISO/IEC 17025 accreditation, approve methods, require incident reporting, and publish performance dashboards.

3. **Quality-first scale-up.** Make accreditation and proficiency testing prerequisites for public funding. Institutionalize method validation, measurement-uncertainty reporting, and inter-lab comparisons.

4. **Digital chain of custody.** Deploy LIMS integrated with ICJS/CCTNS, enforcing tamper-evident packaging, scan-to-chain events, cryptographic hashes for digital media, and automated disclosure logs.

5. **Human capital.** Expand NFSU-State cadet programs, sponsor PhD/post-doc fellowships in statistics and measurement science, and mandate court-facing training (report writing, testimony, statistics for lawyers and judges).

6. **Research and transparency.** Fund independent accuracy/precision studies for pattern-evidence disciplines and publish anonymized quality-metrics (backlogs, TAT, proficiency outcomes) to incentivize improvement and public trust.

7. **Ethics-by-design.** Implement privacy impact assessments for new databases, adopt data-minimization defaults, and establish independent review for sensitive bio-surveillance deployments and AI-enabled forensic tools.

References

1. Indian Evidence Act, 1872 (Act No. 1 of 1872). Government of India.
2. Identification of Prisoners Act, 1920 (Act No. 33 of 1920). Government of India.
3. Code of Criminal Procedure, 1973 (Act No. 2 of 1974). Government of India.
4. Information Technology Act, 2000 (Act No. 21 of 2000). Government of India.
5. National Research Council. (2009). Strengthening Forensic Science in the United States: A Path Forward. National Academies Press.
6. Selvi v. State of Karnataka, (2010) 7 SCC 263 (India).
7. Government of India, Ministry of Health & Family Welfare. (2014). Guidelines & Protocols: Medico-legal care for survivors/victims of sexual violence.
   Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 (India).
8. European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation).

9. President's Council of Advisors on Science and Technology (PCAST). (2016). Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods.

10. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).
Government of India, Ministry of Electronics & Information Technology. (2017). Notification under Section 79A of the IT Act—Examiners of Electronic Evidence.

11. International Organization for Standardization/International Electrotechnical Commission. (2017). ISO/IEC 17025:2017—General requirements for the competence of testing and calibration laboratories.

12. Government of India. (2019). The DNA Technology (Use and Application) Regulation Bill, 2019.

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

14. National Forensic Sciences University Act, 2020 (Act No. 32 of 2020). Government of India.

15. United Kingdom. (2021). Forensic Science Regulator Act 2021.

16. Criminal Procedure (Identification) Act, 2022 (Act No. 11 of 2022) and Rules, 2022. Government of India. National Crime Records Bureau. (2022). Crime in India 2021 (Annual report)