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

VOLUME 5 AND ISSUE 13 OF 2025

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

Published by

Institute of Legal Education

https://iledu.in

ADMISSIBILITY OF FINGERPRINT RECOGNITION EVIDENCE IN INDIAN CRIMINAL TRIALS: AN ICT AND LEGAL PERSPECTIVE

AUTHOR - MAHALAKSHMI V, STUDENT AT THE TAMIL NADU DR. AMBEDKAR LAW UNIVERSITY, SCHOOL OF EXCELLENCE IN LAW

BEST CITATION - MAHALAKSHMI V, ADMISSIBILITY OF FINGERPRINT RECOGNITION EVIDENCE IN INDIAN CRIMINAL TRIALS: AN ICT AND LEGAL PERSPECTIVE, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (13) OF 2025, PG. 539-552, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

The introduction of the National Automated Fingerprint Identification System (NAFIS) and India's new criminal legal framework—comprising the *Bharatiya Sakshya Adhiniyam* (BSA), 2023, and the *Criminal Procedure (Identification) Act* (CPI Act), 2022—has fundamentally shifted fingerprint evidence from a traditional forensic discipline to a high-volume, ICT-enabled domain. This paper undertakes a doctrinal analysis of the legal and technical requirements governing the admissibility of this evidence in Indian criminal trials. It establishes that admissibility now rests on a critical duality: the traditional judicial acceptance of the science as reliable expert opinion (BSA Section 39) must be seamlessly integrated with the stringent procedural standards for **electronic records** (BSA Section 63). Key findings highlight that the constitutionality of the NAFIS database is intrinsically threatened by the CPI Act's mandatory **75-year data retention period**, which is highly vulnerable to challenge under the proportionality test inherent in Article 21. Furthermore, admissibility relies entirely on procedural compliance, specifically the mandatory *Section 63(4) Certificate* (KsandK, 2023), which requires accurate documentation of digital integrity via hash value protocols. The current lack of mandatory algorithm validation and standardized forensic training poses significant technical risks to the evidentiary reliability of automated matches. The paper concludes that without immediate policy reforms to standardize protocols, ensure algorithm transparency and harmonizes retention policies with constitutional mandates, the integrity and continued admissibility of this cornerstone of forensic evidence will remain precarious.

Keywords: Fingerprint Recognition; Automated Fingerprint Identification System (AFIS); National Automated Fingerprint Identification System (NAFIS); Bharatiya Sakshyam Adhiniyam (BSA) 2023; Criminal Procedure (Identification) Act (CPI Act) 2022; Electronic Evidence; Admissibility; Right to Privacy (Article 21); Chain of Custody (CoC); Forensic Science.

1. Introduction

The Indian criminal justice system, historically reliant on manual comparison of physical evidence, is undergoing a profound transformation driven by Information and Communication Technology (ICT) and new legislative mandates. Central to this shift is the **Fingerprint Recognition Evidence**, transitioning from a conventional forensic discipline (*Dactyloscopy*)[897] to a component of large-scale digital identification systems like the National Automated Fingerprint Identification System (NAFIS)[898]. This evolution is governed by the simultaneous enactment of the *Bharatiya Sakshya Adhiniyam* (BSA), 2023, the *Bharatiya Nagarik Suraksha Sanhita* (BNSS), 2023, and the

[897] *Dactyloscopy* is the scientific study of fingerprints for identification purposes
[898] *Criminal Procedure (Identification) Act*, No. 11 of 2022, §§ 2(1)(b), 3 (India).

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

VOLUME 5 AND ISSUE 13 OF 2025

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

Published by

Institute of Legal Education

https://iledu.in

Criminal Procedure (Identification) Act (CPI Act), 2022.

This assignment undertakes a comprehensive doctrinal and technical study of the legal admissibility of fingerprint recognition evidence in this ICT-enabled environment. The central argument is that while fingerprint evidence maintains a high scientific standing—judicially recognised as an "exact science"[899]—its legal admissibility now hinges critically on satisfying the strict procedural and technical integrity requirements for **electronic records** mandated by the BSA, 2023, and surviving constitutional scrutiny regarding mass data retention under the CPI Act, 2022. Failure to adequately bridge the gap between technical complexity and transparent legal procedure threatens the evidentiary value of this cornerstone of forensic science.

2. Technological Foundation and ICT Integration

The shift from magnifying glass analysis to algorithm-driven comparison fundamentally alters the investigative procedure and the standards of proof required in court. Understanding the technological underpinnings of modern systems is therefore essential for assessing legal admissibility.

2.1. What is Fingerprint Recognition System?

A fingerprint recognition system, fundamentally, is a technological process designed to analyse and verify an individual's identity based on the unique, permanent characteristics of their **friction ridge patterns**[900]. A fingerprint itself is an impression left by the papillary ridges on a human finger, formed by the skin's surface structure. The system captures this impression—whether through ink and paper or, more commonly today, through optical or capacitance scanning—and converts it into a digital template for storage and comparison. This technology is a form of biometric identification, leveraging the fact that fingerprints are unique, difficult to alter, and durable over an individual's life[901]. In forensic terms, the system moves beyond mere classification to establishing individual identity through precise comparison.

2.2. How does Fingerprint Recognition System work?

The Automated Fingerprint Identification System (AFIS), or its national iteration, NAFIS, functions through a sequential process involving digital capture, feature extraction, and pattern matching:

1. **Image Acquisition:** This is the process of capturing the fingerprint, typically using Live Scan optical or capacitance devices for known prints (ten-prints) or high-resolution photography and lifting techniques for latent prints recovered from a crime scene[902]. The raw image is digitized and enhanced to remove noise and clarify ridge patterns.
2. **Feature Extraction:** This is the critical analytical step. The system identifies and maps the unique, immutable features within the print known as **minutiae**[903]. Minutiae are specific points on the ridges, primarily:
   - **Ridge Endings:** Where a single friction ridge terminates.
   - **Bifurcations:** Where a single ridge splits into two.

   The system translates the spatial geometry of these minutiae into a numerical or geometrical template (the fingerprint template).
3. **Pattern Matching (Algorithm Comparison):** The extracted template of an unknown print is compared against the database of known templates using complex matching algorithms. This

[899] *Re Govinda Reddy v. State of Mysore*, AIR 1958 Mys 140 (India).

[900] Fingerprint. (n.d.). In *Wikipedia*. Retrieved from https://en.wikipedia.org/wiki/Fingerprint

[901] Fingerprint. (n.d.). In *Wikipedia*. Retrieved from https://en.wikipedia.org/wiki/Fingerprint

[902] Campbell, J. P. (1997). Speaker recognition: A tutorial. *Proceedings of the IEEE, 85*(9), 1437–1462. https://doi.org/10.1109/5.628714

[903] Fingerprint. (n.d.). In *Wikipedia*. Retrieved from https://en.wikipedia.org/wiki/Fingerprint

typically involves a **1:N Search**, where the unknown sample is checked against the entire database (N being the population of stored prints) at immense speeds—tens of thousands of comparisons per second[904]. The algorithm generates a **similarity score** based on the number and spatial congruence of matched minutiae, which determines the ranking of potential candidates.

4. **Decision Making:** The system ranks the candidates by similarity score, often requiring a human expert review to confirm the match based on defined judicial standards (e.g., minimum number of corresponding minutiae points). The final output, presented in court, is based on this high-confidence expert verification of the automated match.

2.3. Types of Fingerprint Recognition System

Fingerprint recognition technologies are classified based on their operational environment and application:

System Type	Description	Application in Indian Investigations
Manual Systems (Dactyloscopy)	Traditional ink-and-paper method, requiring human expert measurement and comparison.	Used for validation, secondary opinion, and in older case records not yet digitized.
Automated Fingerprint Identification Systems (AFIS)	Digital system using algorithms for feature extraction, storage, and 1:**N** searching.	Standard tool in all Central/State Forensic Science Laboratories (CFSLs/FSLs).
National AFIS (NAFIS)	The centralized, integrated national AFIS repository managed by the National Crime Records Bureau (NCRB)[905].	Large-scale database matching, inter-state criminal identification, and data sharing via CCTNS.
Live Scan Systems	Electronic capture devices (optical or capacitance scanners) that produce high-quality digital ten-print records instantly.	Used in police stations and prisons for immediate, high-quality collection of known prints under the CPI Act, 2022.
Latent Print Systems	Systems specifically designed to process, enhance, and search low-quality, partial prints recovered from crime	Crucial for connecting crime scenes to database records (cold case searching).[9]

[904] National Institute of Justice (NIJ). (n.d.). *Automatic fingerprint identification systems (AFIS): Technical report.* U.S. Department of Justice.

[905] Shankarias Parliament. (n.d.). *NCRB and NAFIS integration with CCTNS.* Retrieved from https://shankariasparliament.in

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

VOLUME 5 AND ISSUE 13 OF 2025

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

Published by

Institute of Legal Education

https://iledu.in

	scenes.	

2.4. Application of Fingerprint Recognition System

The applications of modern fingerprint recognition systems are diverse, spanning both forensic science and public security management, fundamentally serving to establish identity and link individuals to crimes:

- **Criminal Identification (1:N Search):** The primary application involves searching an unknown print (e.g., a latent print from a murder weapon) against the NAFIS database to identify a suspect or link a repeat offender to a new crime[906].
- **Case Linkage:** AFIS/NAFIS allows investigating agencies to link seemingly disparate crimes (serial offenses) across different jurisdictions or states by matching unknown prints left at various scenes.
- **Biometric Verification (1:1 Search):** Used to confirm the identity of a known suspect against a stored ten-print card.
- **Access and Security Control:** Although secondary to forensic use, fingerprint biometrics is integrated into secure government facilities and digital systems to verify access, providing secondary evidence in cybercrime cases (e.g., proving unauthorized access to a computer system)[907].
- **Post-mortem Identification:** Used by authorities to identify incapacitated or deceased individuals (e.g., disaster victims) when other forms of identification are unavailable[908].

2.5. Features of Fingerprint Recognition System

The technological features that define AFIS systems are rooted in computational efficiency and biometric stability:

- **Uniqueness and Permanence:** The core scientific feature, ensuring the long-term reliability of the system as an identity marker[909].
- **Indexing and Classification:** AFIS uses algorithms to classify and index prints (e.g., whorl, loop, arch) into manageable groups, significantly speeding up the 1:N comparison search process.
- **Scalability:** The architecture allows for the continuous expansion of the database to accommodate millions of records, making it suitable for national-level systems like NAFIS, which requires handling data from all states and union territories.
- **Interoperability (CCTNS Integration):** NAFIS is designed to integrate with the Crime and Criminal Tracking Network System (CCTNS), [n] enabling police across the country to access fingerprint identification as part of a seamless digital investigation ecosystem.
- **Template Generation:** The system stores minimal data required for comparison—the minutiae map and pattern type—rather than the full image. This template is quicker to process and potentially more secure if stored properly.

2.6. Advantages and Disadvantages

The move towards ICT-enabled fingerprint analysis brings profound benefits to criminal investigation but introduces significant judicial and technical risks.

2.6.1. Advantages

1. **High Reliability and Scientific Standing:** Fingerprint evidence is considered scientific and objective, enjoying high

[906] National Institute of Justice (NIJ). (n.d.). *Automatic fingerprint identification systems (AFIS): Technical report.* U.S. Department of Justice.
[907] *Bharatiya Sakshya Adhiniyam*, No. 46 of 2023, §§ 2, 4; *Information Technology Act*, No. 21 of 2000, §§ 2, 4 (India).
[908] Fingerprint. (n.d.). In *Wikipedia*. Retrieved from https://en.wikipedia.org/wiki/Fingerprint
[909] Fingerprint. (n.d.). In *Wikipedia*. Retrieved from https://en.wikipedia.org/wiki/Fingerprint

reliability in forensic science. It has been recognised by the judiciary as advanced to an "exactitude level"[910], which aids its admissibility under expert opinion.

2. **Automation and Speed:** AFIS/NAFIS enables investigators to conduct searches that were previously impossible due to scale. Automated comparison rapidly filters candidates, enhancing investigative efficiency and reducing case backlog[911].
3. **Non-Invasive Biometric:** Compared to biological samples (like DNA), fingerprint collection is generally seen as non-invasive and falls within the scope of **non-testimonial compulsion** under Article 20(3)[912], reducing constitutional hurdles during collection.
4. **Long-Term Identifier:** Due to the permanence of the ridge patterns, a master print collected today can reliably identify an individual decades later, supporting the 75-year retention mandate of the CPI Act, 2022.

2.6.2. Disadvantages

1. **Dependence on Data Quality:** Automated matching is only as reliable as the input. Low-quality latent prints (smudged, partial, or obscured) significantly increase the False Acceptance Rate (FAR) or False Rejection Rate (FRR).[913] This compromises the algorithmic reliability and subsequent court testimony.
2. **Lack of Statistical Foundation:** Academic critiques argue that the error rate in AFIS matching has not been adequately studied or validated to provide a secure statistical foundation for infallibility, especially concerning the probabilistic output of algorithms[914]. This challenges the judicial assumption that the science is always "exact" in a digital context.
3. **Risk of Bias:** Research suggests that even the subsequent human expert review of AFIS candidates is not entirely immune to **contextual bias** (being swayed by extraneous information about the suspect).[915]
4. **Digital Vulnerabilities:** As electronic records, fingerprint templates stored in NAFIS are vulnerable to hacking, unauthorized access, or malicious alteration and duplication, especially given the prolonged 75-year retention period.[916] This necessitates stringent security measures under the IT Act, 2000, and the new data protection norms.
5. **Interoperability Challenges:** Varying standards of capture devices and software across different State FSLs pose challenges for seamless cross-jurisdictional comparison within the NAFIS network.[917]

3. The Legal Framework of Admissibility

The admissibility of fingerprint evidence in India is governed by a robust, multi-layered legal framework that combines constitutional rights, new criminal procedure, and updated evidence laws.

3.1. Overview of Indian laws on Fingerprint recognition

3.1.1. Constitutional mandates: Article 20(3) and Article 21

The compulsion to provide fingerprint biometrics must align with fundamental rights, primarily the right against self-incrimination and the right to privacy.

- **Article 20(3) (Right against Self-Incrimination):** This article states that "no person accused of any offence shall be

[910] *Re Govinda Reddy v. State of Mysore*, AIR 1958 Mys 140 (India).
[911] National Institute of Justice (NIJ). (n.d.). *Automatic fingerprint identification systems (AFIS): Technical report.* U.S. Department of Justice.
[912] *Ritesh Sinha v. State of Uttar Pradesh*, (2019) 8 SCC 1 (India).
[913] Mitretek Systems. (n.d.). *The role of data quality in biometric systems.* National Institute of Justice Technical Report.
[914] Himachal Pradesh National Law University (HPNLU). (n.d.). *Legal challenge analysis: Criminal Procedure (Identification) Act, 2022.*
[915] Fingerprint evidence. (n.d.). In *Wikipedia.* Retrieved from https://en.wikipedia.org/wiki/Fingerprint
[916] Himachal Pradesh National Law University (HPNLU). (n.d.). *Legal challenge analysis: Criminal Procedure (Identification) Act, 2022.*
[917] ResearchGate. (n.d.). *Utilizing new technologies to solve problems of evidence.* Retrieved from https://www.researchgate.net

compelled to be a witness against himself." The Supreme Court, in its reasoning concerning similar biometrics (voice samples) in *Ritesh Sinha v. State of Uttar Pradesh*[918], clarified that compelling a person to provide a physical attribute, such as a fingerprint, does **not** amount to self-incrimination. Fingerprints are considered **non-testimonial compulsion** because they are physical characteristics used only for comparison, not for revealing conscious knowledge or mental thought[919]. This constitutional interpretation provides the foundational legality for the compulsory collection powers under the CPI Act, 2022.

- **Article 21 (Right to Life and Personal Liberty/Privacy):** The right to privacy, affirmed in *Justice K.S. Puttaswamy v. Union of India*, [920] dictates that any state action that intrudes upon personal data, such as the mass collection and retention of biometrics, must meet the three-part **Proportionality Test**: the action must be lawful, pursue a legitimate state aim, and be proportional to that aim.

The CPI Act, 2022, faces severe constitutional challenges specifically on the grounds of proportionality, primarily due to its **mandatory 75-year retention period** of biometrics, including fingerprints, even after acquittal[921]. Critics argue this prolonged retention lacks a "reasonable nexus" with the objective of investigation, increases the "probability of malicious use," and violates the right to privacy by being overly burdensome on the acquitted individual, thus failing the proportionality test under Article 21.[922]

3.1.2. Bharatiya Sakshya Adhiniyam (BSA), 2023

The BSA, replacing the Indian Evidence Act, 1872, is the primary statute governing the admissibility and weight of fingerprint evidence, establishing two distinct legal pathways:

- **Section 39 (Expert Opinion):** This section supersedes the old Section 45 and confirms that the **opinion of an expert in finger impressions** is a valid and admissible form of expert evidence in court[923]. This covers the traditional method of forensic analysis and comparison. The expert is crucial for interpreting the AFIS match score and testifying on the scientific basis of the identification.
- **Sections 62 and 63 (Electronic Records):** Since AFIS reports, digital images, and NAFIS data are electronic records or "computer output," they must satisfy the specific requirements of the BSA for digital evidence[924]. **Section 63(4)** mandates the production of a **Certificate** from a person managing the computer device or activity, attesting to the integrity and authenticity of the electronic record. This certificate must confirm that the AFIS system was operating correctly and the data was regularly and accurately fed into the system[925]. This certification is mandatory and failure to produce a proper Section 63(4) certificate can render technically sound AFIS evidence inadmissible.

3.1.3. Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023

The BNSS (replacing the CrPC) provides the procedural authority and context for the collection and handling of evidence, working in tandem with the CPI Act, 2022. The BNSS governs the investigative process, dictating how the Investigating Officer (IO) must lawfully obtain and preserve the fingerprint sample, thus ensuring a valid **Chain of Custody** (CoC) which is essential for admissibility[926].

[918] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).
[919] *Ritesh Sinha v. State of Uttar Pradesh*, (2019) 8 SCC 1 (India).
[920] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).
[921] HPNLU. (n.d.). *Legal challenge analysis: CPI Act, 2022 — Retention period critique.*
[922] Himachal Pradesh National Law University (HPNLU). (n.d.). *Legal challenge analysis: Criminal Procedure (Identification) Act, 2022.*
[923] Hawkeye Forensic. (n.d.). *Expert opinion under Section 39 of Bharatiya Sakshya Adhiniyam, 2023.* Retrieved from https://www.hawkeyeforensic.com
[924] *Bharatiya Sakshya Adhiniyam*, No. 46 of 2023, §§ 62, 63, 39, 72 (India).
[925] Ministry of Home Affairs. (2023). *Certificate procedure under Section 63 of Bharatiya Sakshya Adhiniyam, 2023.*
[926] National Judicial Academy. (n.d.). *Digital forensics and chain of custody: Training presentation.*

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

VOLUME 5 AND ISSUE 13 OF 2025

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

Published by

Institute of Legal Education

https://iledu.in

3.1.4. The Criminal Procedure (Identification) Act, 2022

The CPI Act, 2022, is the foundational law for the physical collection of biometrics. It significantly expands the scope compared to the prior Identification of Prisoners Act, 1920:

- **Scope of Measurements:** The term "Measurements" is defined to explicitly include finger impressions, palm prints, foot impressions, and biological samples, granting police and prison officers the power of compulsory collection from convicts, arrested persons, and those detained under preventive laws[927].
- **Compulsory Collection:** For specific serious offenses, measurements may be taken *without consent*, allowing for forceful collection if necessary[928].
- **Data Retention:** The Act mandates that these digital records must be retained for **seventy-five years**, and places the onus on the individual (if acquitted) to apply for the destruction of their records[929]. This prolonged retention and the burden of requesting destruction are the key points of constitutional friction under Article 21[930].

3.1.5. Information Technology Act (IT Act), 2000

The IT Act, 2000, provides the general legal framework for electronic transactions and digital security in India.

- **Sensitive Personal Data:** The IT Rules, 2011, categorize biometric data, including fingerprints, as **Sensitive Personal Data or Information (SPDI)**[931]. This classification mandates specific data protection requirements, including informed consent and stringent security safeguards, which are vital for the integrity of the NAFIS database.
- **Digital Integrity:** Sections of the IT Act regarding unauthorized access, hacking, and breach of confidentiality indirectly contribute to the legal framework for the security and authenticity of digital evidence stored in AFIS systems[932]. Any successful breach or tampering of the NAFIS database could invoke both civil and criminal liabilities under the IT Act.

3.2. Admissibility criteria of fingerprint recognition evidence in India

The admissibility of modern fingerprint evidence is determined by the successful synthesis of both forensic science standards and digital integrity protocols.

Admissibility Criterion	Description	Governing Statute/Principle
Relevance	The fingerprint must be clearly connected to the facts in issue (e.g., placing the accused at the crime scene).	BSA, 2023 (Sections 4-7)
Expert Competence	The comparison and analysis must be conducted by a qualified and accredited fingerprint expert	BSA, 2023 (Section 39)[933]

[927] PRS Legislative Research. (2022). *Bill summary: Criminal Procedure (Identification) Act, 2022*. Retrieved from https://prsindia.org
[928] Ibid
[929] Ibid
[930] Himachal Pradesh National Law University (HPNLU). (n.d.). *Legal challenge analysis: Criminal Procedure (Identification) Act, 2022.*
[931] Kuey.net. (n.d.). *IT Act, 2000: Sensitive personal data and biometric classification.* Retrieved from https://kuey.net
[932] The Law Institute. (n.d.). *Information Technology Act, 2000: Data protection and privacy overview.*
[933] Hawkeye Forensic. (n.d.). *Expert opinion under Section 39 of Bharatiya Sakshya Adhiniyam, 2023*. Retrieved from https://www.hawkeyeforensic.com

	(forensic scientist).	
Clarity and Quality	The print must be sufficiently clear to allow the expert and the court to confirm minutiae matching (especially important for latent prints).	Judicial precedent (*Govinda Reddy*[934]), technical validation.
Lawful Acquisition	The sample must be collected according to the procedural authority granted by the CPI Act, 2022, and the BNSS, 2023.	CPI Act, 2022[935]; BNSS, 2023.
Unbroken Chain of Custody (CoC)	Meticulous documentation tracking the fingerprint sample (physical or digital file) from seizure to submission, ensuring no contamination or alteration.	BNSS, 2023; Judicial mandate[936]
Mandatory Certification	For any digital output (AFIS report, digital image), a Section 63(4) certificate confirming the integrity and operational accuracy of the computer system is compulsory.	BSA, 2023 (Section 63)[4,20]
Hash Value Integrity	Authentication of the electronic record by logging the hash value—a unique digital fingerprint of the file—at every transfer point to prove non-alteration.	BSA, 2023 (Section 63)[20]

3.3. Judicial Interpretation

Indian courts have traditionally treated fingerprint evidence with immense respect, setting precedents that affirm its high evidentiary value but also mandate strict scrutiny of its presentation.

- ***Re Govinda Reddy v. State of Mysore* (1958) – The "Exact Science" Doctrine:** This landmark judgment established the seminal judicial principle that the science

[934] *Re Govinda Reddy v. State of Mysore*, AIR 1958 Mys 140 (India).
[935] PRS Legislative Research. (2022). *Bill summary: Criminal Procedure (Identification) Act, 2022*. Retrieved from https://prsindia.org
[936] National Judicial Academy. (n.d.). *Digital forensics and chain of custody: Training presentation.*

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 13 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

of fingerprint comparison has advanced to a level of **"exactitude"**[937]. This ruling forms the foundational acceptance of fingerprint evidence as highly reliable, providing the basis for its inclusion under the expert opinion statutes.

- ***Bhaluka Behara and others v. State* – Judicial Duty to Confirm:** Building upon the *Govinda Reddy* principle, this ruling clarified that even after receiving expert testimony; the court retains the duty to confirm the expert's findings by comparing the enlarged prints themselves and applying its own judgment to determine similarity or dissimilarity[938]. This is a crucial safeguard, preventing the court from becoming a mere rubber stamp for the expert.
- ***State of U.P. v. Ram Babu Misra* (1980) – The Corroboration Principle:** While fingerprint evidence is powerful, the Supreme Court has often urged caution, emphasizing that expert evidence should be **corroborated** with other circumstantial evidence (like witness statements or confessions) before basing a conviction solely on the expert's opinion[939]. This ensures holistic proof and higher evidentiary certainty.
- **Warning Against the "Aura of Infallibility":** In appreciating complex scientific evidence, the Supreme Court has warned that advanced techniques can create an **"aura of infallibility,"** potentially causing human judgment to be clouded by the perceived certainty of the technology[940]. This judicial caution is highly relevant in the AFIS era, where the speed and complexity of the algorithm might discourage the necessary judicial skepticism.

4. ICT Enabled Investigation Practices

The integration of advanced ICT into forensic science has created new possibilities for leveraging fingerprint data in criminal investigations, but this practice is only as strong as the security and reliability of the underlying systems.

4.1. Forensic application in Fingerprint Recognition

Forensic application of modern fingerprint recognition relies heavily on automated and digital tools:

- **Latent Print Processing:** Crime scene units use advanced chemical and digital enhancement techniques (like high-resolution scanners and specialized software) to lift and process latent prints, which are then digitized for AFIS input.
- **AFIS Search and Matching:** The primary application is the 1:N search on NAFIS, where the automated algorithm compares the questioned latent print against the massive database of known ten-prints, utilizing minutiae mapping to generate candidate lists[7].
- **Establishing Individuality:** The forensic expert's task, post-AFIS match, is to establish the individuality of the suspect by confirming the sufficient number of matching minutiae points between the latent print and the known sample, a crucial step for admissibility under BSA Section 39.

4.2. Institutions involved in India for Fingerprint Recognition

The system requires coordination between technical database managers, investigative agencies, and forensic analysis bodies:

- **National Crime Records Bureau (NCRB):** The central agency responsible for rolling out and managing the **NAFIS** database. The NCRB maintains the centralized repository and is tasked with specifying the guidelines for handling, storage, processing, and disposal of the records

[937] *Re Govinda Reddy v. State of Mysore*, AIR 1958 Mys 140 (India).
[938] Ibid.
[939] LawGratis. (n.d.). *Fingerprint evidence and corroboration in Indian courts.* Retrieved from https://lawgratis.in
[940] *R. v. Beland*, [1987] 2 SCR 398 (Can.), cited in *Indian Supreme Court Judgment* (Ritesh Sinha v. State of U.P., 2019).

collected under the CPI Act, 2022[941]. The NCRB is crucial for providing the digital integrity (Part A of the Sec 63 certificate) for the NAFIS system itself.

- **Central Forensic Science Laboratories (CFSLs) and State FSLs:** These accredited labs provide the expert testimony under BSA Section 39. They perform the final, human-verified comparison of the prints (post-AFIS filtering) and issue the expert reports, often responsible for providing the technical inputs required for the BSA Section 63(4) certificate (Part B)[942].
- **Bureau of Police Research and Development (BPR&D):** Involved in capacity building and developing standardized training modules for police officers on biometric collection and digital evidence preservation.
- **Police/Prison Authorities:** Authorized under the CPI Act, 2022, and BNSS, 2023, to perform the initial collection of measurements (live scan captures) and maintain the physical and digital **Chain of Custody** during the investigation phase.

4.3. ICT integration with other tools

Fingerprint data is increasingly valuable when integrated into the broader digital investigation ecosystem:

- **CCTNS and NATGRID:** NAFIS is being integrated with the Crime and Criminal Tracking Network System (CCTNS)[943] and the National Intelligence Grid (NATGRID). This allows police to cross-reference fingerprint matches with non-biometric data—such as Call Detail Records (CDRs), geo-location data, and CCTV metadata—to establish a comprehensive digital trail of the suspect.
- **Digital Forensic Tools:** Fingerprint data recovered from digital carriers (e.g., hard drives containing malicious files with a user's print used for authentication) are analysed using digital forensic software (like FTK or EnCase) to link the digital activity to the authenticated identity.
- **Biometric Cross-referencing:** AFIS output is often cross-referenced with other biometric databases (e.g., facial recognition systems, or, where permitted, Aadhaar-linked systems) to build a multi-layered identity profile.

4.4. Reliability and Security

The admissibility of digital AFIS output under BSA Section 63 demands demonstrable reliability of the system and stringent security of the stored data.

4.4.1. Reliability

Reliability, in the ICT context, moves beyond the scientific uniqueness of the ridge patterns to the operational accuracy of the software:

- **Accuracy and Error Rates (FAR/FRR):** Courts must be satisfied that the AFIS system performs within acceptable, independently tested error parameters (False Acceptance Rate and False Rejection Rate)[944]. Un-validated algorithms pose a significant risk to the integrity of the evidence.
- **Validation and Standardization:** The system and the analysis methodologies used by CFSLs must be empirically validated according to national (BIS) and international standards (e.g., ISO/IEC 19795) to ensure consistent performance across all labs[945].
- **Expert Explanation:** The expert witness must clearly explain the system's limitations, the comparison method used, the degree of certainty, and the margin of

[941] PRS Legislative Research. (2022). *Bill summary: Criminal Procedure (Identification) Act, 2022*. Retrieved from https://prsindia.org
[942] *Bharatiya Sakshya Adhiniyam*, No. 46 of 2023, §§ 62, 63, 39, 72 (India).
[943] NCRB. (n.d.). *Proposal for integrating CCTNS with CFPB under NAFIS initiative*.
[944] Mitretek Systems. (n.d.). *The role of data quality in biometric systems*. National Institute of Justice Technical Report.
[945] International Organization for Standardization (ISO). (2006). *ISO/IEC 19795: Biometric performance testing and reporting*. Geneva: ISO.

error to the court, as mandated by judicial precedent[946].

4.4.2. Security

The immense, long-term repository of sensitive personal data (NAFIS) necessitates robust security protocols:

- **Data Encryption:** Digital fingerprint templates must be encrypted both *in transit* (during transfer from police station to NAFIS server) and *at rest* (in the database) to prevent interception or unauthorized access[947].
- **Access Control and Audit Trails:** Strict, role-based access control must be implemented, ensuring only authorized personnel (IOs, FSL analysts) can retrieve data. Crucially, the system must maintain detailed **audit logs** to track every access, modification, or search operation, providing the necessary trail for judicial review of integrity[948].
- **Integrity Verification (Hash Values):** The use of cryptographic **Hash Values** is indispensable. A unique hash must be computed and logged at the point of capture, transfer, and analysis. If the hash changes, it provides irrefutable proof that the electronic file has been altered or tampered with, undermining the Section 63 certification and rendering the evidence inadmissible[949].
- **Cybersecurity of the ICT Infrastructure:** The NAFIS infrastructure must be protected against external cyber threats (hacking, ransomware)[950] and insider threats, given the sensitive nature of the biometric data and the long retention period (75 years)[951].

5. Challenges and Recommendations in the ICT Era

The legal and technical integration of digital fingerprint evidence presents several acute challenges that must be overcome to fully realise the potential of NAFIS while maintaining constitutional legality and evidentiary fairness.

5.1. Challenges

5.1.1. Constitutional and Privacy Overreach

The mandatory **75-year retention period** under the CPI Act, 2022, remains the most significant legal and constitutional challenge. This long retention, particularly for individuals who are acquitted or discharged, is challenged under Article 21, as it is disproportionate to the legitimate state aim of criminal identification[952]. Furthermore, the lack of a dedicated, robust data protection framework exacerbates the risk of misuse, abuse, and data breaches for this highly sensitive biometric data[953].

5.1.2. Lack of Standardization and Validation

A key scientific challenge is the absence of **uniform forensic protocols** across all CFSLs and State FSLs for the handling and analysis of digital prints. This inconsistency can lead to variations in results depending on the laboratory or the expert, undermining the "exact science" doctrine[954]. Critically, NAFIS algorithms lack mandatory, independent third-party scientific validation, meaning their specific error rates (FAR/FRR) are not transparently known or judicially verifiable, complicating the assessment of reliability in court[955].

5.1.3. Procedural Compliance Gaps

The stringent requirement of the **BSA Section 63(4) Certificate** is a major procedural bottleneck. IOs and FSL staff often lack the specialized training to generate the highly technical metadata, hash logs, and detailed

[946] *Ram Singh v. Col. Ram Singh*, AIR 1986 SC 3 (India).
[947] Unique Identification Authority of India (UIDAI). (2021). *Guidelines on encryption and security of biometric data.*
[948] National Crime Records Bureau (NCRB). (2022). *Guidelines on data protection in CCTNS systems.*
[949] Ministry of Home Affairs. (2023). *Certificate procedure under Section 63 of Bharatiya Sakshya Adhiniyam, 2023.*
[950] Ministry of Home Affairs, Cyber Security Cell. (2021). *Audit report on law enforcement IT systems.*
[951] Himachal Pradesh National Law University (HPNLU). (n.d.). *Legal challenge analysis: Criminal Procedure (Identification) Act, 2022.*
[952] Himachal Pradesh National Law University (HPNLU). (n.d.). *Legal challenge analysis: Criminal Procedure (Identification) Act, 2022.*
[953] *Data protection challenges and risks of biometric data abuse in India.*
[954] Directorate of Forensic Science Services (DFSS). (2022). *Internal audit report on laboratory practices.*
[955] Mitretek Systems. (n.d.). *The role of data quality in biometric systems.* National Institute of Justice Technical Report.

system information required for the two-part certification process[956]. This capacity gap means that even a perfectly valid fingerprint match may be legally excluded due to defective electronic evidence certification[957].

5.1.4. Digital Tampering and Forgery Risks

Although fingerprints are physically durable, their digital representation is vulnerable. Advanced digital editing software can manipulate latent print images or minutiae maps. Furthermore, the use of AI/Deepfake technology, while not yet widely publicised for fingerprints as it is for voice, raises the future spectre of **synthetic print generation**, which could be used to falsely incriminate or create misleading digital evidence[958].

5.1.5. Infrastructure and Capacity Deficit

For NAFIS to function effectively nationwide, there must be a massive upgrade in the infrastructure of forensic and scientific laboratories and a substantial expansion of the workforce trained in digital forensics. Currently, the capacity of many labs and the technical training levels of the general police force remain inadequate for handling the scale and complexity of the new ICT-enabled evidence standards[959].

5.2. Recommendations

To ensure that the benefits of ICT-enabled fingerprint recognition are fully integrated without compromising the principles of a fair trial and constitutional rights, immediate and focused reforms are required:

1. **Enact Statutory Data Protection Framework:** The government must urgently establish a specific data protection framework for biometric data (potentially leveraging the Digital Personal Data Protection Act, 2023)[960]. This framework must mandate:
    - **Proportional Retention Limits:** Replacing the 75-year mandate with constitutionally proportionate limits, especially for acquitted individuals.
    - **Accountability:** Clear mechanisms to hold the NCRB accountable for data breaches or non-destruction of records upon acquittal.
    - **Mandatory Audit Trails:** Systemic requirements for auditable logs of all access to the NAFIS database.
2. **Establish Independent Algorithm Validation:** An independent scientific authority (such as a specialized wing of the DFSS or a national standards body) must be mandated to:
    - **Audit NAFIS Algorithms:** Regularly audit the matching algorithms to certify and publicly disclose certified error rates (FAR/FRR) of the system[961].
    - **Standardize SOPs:** Formulate and enforce uniform national Standard Operating Procedures (SOPs) for digital fingerprint analysis across all CFSLs and FSLs, ensuring consistency and reliability[962].
3. **Mandate BSA Section 63 Capacity Building:** Focused and certified training programs must be developed for Investigating Officers and Forensic Analysts on the precise requirements of the BSA Section 63(4) certificate. This training must cover:
    - **Hash Value Protocol:** Mandatory use and logging of hash values for every digital evidence transfer.
    - **Metadata Preservation:** Detailed preservation of all necessary system metadata for the two-part certification

[956] Ministry of Home Affairs. (2023). *Certificate procedure under Section 63 of Bharatiya Sakshya Adhiniyam, 2023.*
[957] Ibid.
[958] National Cyber Security Coordinator Office. (2023). *Advisory on deepfake voice threats.*
[959] *Need for forensic infrastructure and officer training expansion in India.*
[960] *Digital Personal Data Protection Act*, No. 22 of 2023 (India).
[961] Fingerprint evidence. (n.d.). In *Wikipedia.* Retrieved from https://en.wikipedia.org/wiki/Fingerprint
[962] Directorate of Forensic Science Services (DFSS). (2022). *Internal audit report on laboratory practices.*

(Part A by the device manager, Part B by the forensic expert)[963].

4. **Invest in Anti-Forgery and Anti-Tampering Tools:** Fund research and procurement of indigenous forensic tools capable of detecting digital manipulation, enhancement artefacts, and potential synthetic fingerprint evidence, thus securing the integrity of the evidence presented in court[964].

5. **Legislative Clarification on Admissibility of Automated Output:** Judicial guidelines should be issued to clarify the specific standards required for automated AFIS matches, distinguishing the reliance placed on the algorithmic score versus the final human expert verification. This prevents the court from being misled by the "aura of infallibility" associated with complex technology[965].

6. Conclusion

The admissibility of Fingerprint Recognition Evidence in Indian criminal trials stands at the crucial intersection of scientific certainty and digital vulnerability. The BSA, 2023, has correctly established a dual standard for this evidence: its scientific acceptance as an **expert opinion** (Section 39) and its necessity as an **electronic record** authenticated by certification (Section 63).

While the CPI Act, 2022, provides the procedural power for the creation of the national NAFIS database, the constitutional challenges related to the 75-year data retention and the significant technical challenges—particularly the lack of algorithm transparency and procedural compliance gaps in generating the BSA Section 63 certificate—represent the most significant threats to admissibility.

Moving forward, the successful integration of fingerprint biometrics depends less on the science (which is fundamentally sound) and more on the **procedural integrity and legal transparency** of the ICT infrastructure. India must prioritize harmonizing its legal framework with its technical ambitions, ensuring rigorous data protection, system validation, and comprehensive capacity building for law enforcement. Only through this disciplined approach can the Indian judiciary continue to rely on fingerprint recognition evidence as a just and unimpeachable pillar of proof.

References:

I. Case Laws

1. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).
2. *Ram Singh v. Col. Ram Singh*, AIR 1986 SC 3 (India).
3. *Re Govinda Reddy v. State of Mysore*, AIR 1958 Mys 140 (India).
4. *Ritesh Sinha v. State of Uttar Pradesh*, (2019) 8 SCC 1 (India).
5. *R. v. Beland*, [1987] 2 SCR 398 (Can.), cited in *Indian Supreme Court Judgment (Ritesh Sinha v. State of U.P., 2019).*

II. Statutes and Official Guidelines

6. *Bharatiya Sakshya Adhiniyam*, No. 46 of 2023, §§ 2, 4; *Information Technology Act*, No. 21 of 2000, §§ 2, 4 (India).
7. *Bharatiya Sakshya Adhiniyam*, No. 46 of 2023, §§ 62, 63, 39, 72 (India).
8. *Criminal Procedure (Identification) Act*, No. 11 of 2022, §§ 2(1)(b), 3 (India).
9. *Digital Personal Data Protection Act*, No. 22 of 2023 (India).
10. Himachal Pradesh National Law University (HPNLU). (n.d.). *Legal challenge analysis: Criminal Procedure (Identification) Act, 2022.*
11. HPNLU. (n.d.). *Legal challenge analysis: CPI Act, 2022 — Retention period critique.*

[963] Ministry of Home Affairs. (2023). *Certificate procedure under Section 63 of Bharatiya Sakshya Adhiniyam, 2023.*
[964] National Cyber Security Coordinator Office. (2023). *Advisory on deepfake voice threats.*
[965] R. *v. Beland*, [1987] 2 SCR 398 (Can.), cited in *Indian Supreme Court Judgment* (Ritesh Sinha v. State of U.P., 2019).

12. Ministry of Home Affairs. (2023). *Certificate procedure under Section 63 of Bharatiya Sakshya Adhiniyam, 2023.*
13. Ministry of Home Affairs, Cyber Security Cell. (2021). *Audit report on law enforcement IT systems.*
14. National Crime Records Bureau (NCRB). (2022). *Guidelines on data protection in CCTNS systems.*
15. National Cyber Security Coordinator Office. (2023). *Advisory on deepfake voice threats.*
16. National Judicial Academy. (n.d.). *Digital forensics and chain of custody: Training presentation.*
17. PRS Legislative Research. (2022). *Bill summary: Criminal Procedure (Identification) Act, 2022.* Retrieved from https://prsindia.org
18. Unique Identification Authority of India (UIDAI). (2021). *Guidelines on encryption and security of biometric data.*

III. Standards and Technical Documents

19. International Organization for Standardization (ISO). (2006). *ISO/IEC 19795: Biometric performance testing and reporting.* Geneva: ISO.
20. Mitretek Systems. (n.d.). *The role of data quality in biometric systems.* National Institute of Justice Technical Report.
21. National Institute of Justice (NIJ). (n.d.). *Automatic fingerprint identification systems (AFIS): Technical report.* U.S. Department of Justice.
22. National Crime Records Bureau (NCRB). (n.d.). *Proposal for integrating CCTNS with CFPB under NAFIS initiative.*
23. Directorate of Forensic Science Services (DFSS). (2022). *Internal audit report on laboratory practices.*
24. Hawkeye Forensic. (n.d.). *Expert opinion under Section 39 of Bharatiya Sakshya Adhiniyam, 2023.* Retrieved from https://www.hawkeyeforensic.com

IV. Academic and Research Sources

25. Campbell, J. P. (1997). *Speaker recognition: A tutorial. Proceedings of the IEEE, 85*(9), 1437–1462. https://doi.org/10.1109/5.628714
26. Togneri, R., & Pullella, J. (2011). *An overview of speaker identification: Accuracy and robustness issues. IEEE Circuits and Systems Magazine, 1*(23). https://doi.org/10.1109/MCAS.2011.941854
27. ResearchGate. (n.d.). *Utilizing new technologies to solve problems of evidence.* Retrieved from https://www.researchgate.net
28. Shankarias Parliament. (n.d.). *NCRB and NAFIS integration with CCTNS.* Retrieved from https://shankariasparliament.in
29. Fingerprint. (n.d.). In *Wikipedia*. Retrieved from https://en.wikipedia.org/wiki/Fingerprint
30. Fingerprint evidence. (n.d.). In *Wikipedia*. Retrieved from https://en.wikipedia.org/wiki/Fingerprint
31. LawGratis. (n.d.). *Fingerprint evidence and corroboration in Indian courts.* Retrieved from https://lawgratis.in
32. Kuey.net. (n.d.). *IT Act, 2000: Sensitive personal data and biometric classification.* Retrieved from https://kuey.net
33. The Law Institute. (n.d.). *Information Technology Act, 2000: Data protection and privacy overview.*
34. Data protection challenges and risks of biometric data abuse in India. (n.d.).
35. Challenges in digital evidence handling and forensic voice training. (n.d.).
36. Need for forensic infrastructure and officer training expansion in India. (n.d.).