



INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 6 AND ISSUE 9 OF 2026

INSTITUTE OF LEGAL EDUCATION



INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN – 2583-2344

(Open Access Journal)

Journal's Home Page – <https://ijlr.iledu.in/>

Journal's Editorial Page – <https://ijlr.iledu.in/editorial-board/>

Volume 6 and Issue 9 of 2026 (Access Full Issue on – <https://ijlr.iledu.in/volume-6-and-issue-9-of-2026/>)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 73059 14348 – info@iledu.in / Chairman@iledu.in



© Institute of Legal Education

Copyright Disclaimer: All rights are reserve with Institute of Legal Education. No part of the material published on this website (Articles or Research Papers including those published in this journal) may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher. For more details refer <https://ijlr.iledu.in/terms-and-condition/>

BIOMETRICS IN CRIMINALISTICS AND SCIENTIFIC INVESTIGATION

AUTHOR – G R RADHIKA, STUDENT AT THE TAMILNADU DR.AMBEDKAR LAW UNIVERSITY SCHOOL OF EXCELLENCE IN LAW

BEST CITATION – G R RADHIKA, BIOMETRICS IN CRIMINALISTICS AND SCIENTIFIC INVESTIGATION, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (9) OF 2026, PG. 531-545, APIS – 3920 – 0001 & ISSN – 2583-2344.

I. INTRODUCTION

Criminalistics—the scientific examination of physical evidence for use in criminal proceedings—has been transformed more dramatically in the past three decades than in any comparable period since Locard articulated the principle that every contact leaves a trace.⁹⁰⁵ At the centre of that transformation is biometric technology: systems that capture, store, and analyse the unique physical and behavioural characteristics of human beings for the purpose of identification. Fingerprints, DNA profiles, iris patterns, facial geometry, voice signatures—each of these has moved from specialist laboratory technique to routine investigative tool, deployed across Indian police stations, forensic science laboratories, border checkpoints, and courtrooms.

The scale of this deployment is worth pausing over. India operates the world's largest biometric identity database through Aadhaar, which has enrolled over 1.3 billion people.⁹⁰⁶ The National Crime Records Bureau maintains a growing database of fingerprint, DNA, and increasingly facial recognition records linked to criminal proceedings.⁹⁰⁷ The Criminal Procedure (Identification) Act, 2022 has expanded what the state can collect, from whom, and for how long—replacing a 1920 law that covered only fingerprints and footprints with one that reaches to iris scans, blood samples, and behavioural measurements.⁹⁰⁸ And the three new criminal law statutes—the Bharatiya Nyaya Sanhita (BNS), the Bharatiya Nagarik Suraksha Sanhita (BNSS), and the Bharatiya Sakshya Adhiniyam (BSA)—have rewritten the procedural and evidentiary framework within which all of this data is collected, processed, and placed before courts.⁹⁰⁹

The legal and policy questions this raises are not peripheral concerns for specialists. They go to the heart of how India balances the legitimate demands of effective crime investigation against the constitutional rights of everyone who comes into contact with the system. The Supreme Court settled the constitutional baseline in *Justice K.S. Puttaswamy v. Union of India*,⁹¹⁰ establishing privacy as a fundamental right under Article 21. But constitutional principles, however clearly stated, do not enforce themselves. The question is whether the statutes, rules, and institutional arrangements that govern biometrics in Indian criminal justice are actually adequate to the task.

This paper makes the case that they are not—at least not yet. The scientific and investigative power of biometric technology is real, and its contribution to criminal justice is substantial. But the legal framework has consistently lagged behind the technology it is meant to govern, and the gaps that have opened up carry serious consequences for privacy, due process, and the rights of marginalised communities. The paper works through the science, the law, and the policy in sequence, with a view to identifying precisely where reform is most urgently needed.

⁹⁰⁵Locard, Edmond, "L'analyse des poussières en criminalistique," *Revue Internationale de Criminalistique* (1929); see generally Paul L. Kirk, *Crime Investigation: Physical Evidence and the Police Laboratory* (1953).

⁹⁰⁶Unique Identification Authority of India, *Annual Report 2022–23* (2023).

⁹⁰⁷National Crime Records Bureau, *Crime in India Report 2022* (Ministry of Home Affairs 2023).

⁹⁰⁸Criminal Procedure (Identification) Act, No. 11 of 2022 (India).

⁹⁰⁹Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023 (India).

⁹¹⁰*K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (India).

II. BIOMETRICS: DEFINITION AND SCIENTIFIC FOUNDATIONS

The term "biometrics" is used in two related but distinct senses. In the broader scientific literature, it refers to the application of statistical methods to biological data. In the context that concerns this paper—identification technology and criminal investigation—it refers specifically to automated systems that measure unique human characteristics and use those measurements to verify or establish identity. The two senses are connected: biometric identification systems are, at their core, statistical systems that express the probability that a measured characteristic matches a stored reference to a defined degree of confidence.

The scientific basis for biometric identification rests on two properties: **universality** (every person possesses the characteristic being measured) and **uniqueness** (the characteristic differs sufficiently between individuals that the probability of two people sharing the same measurement is negligibly small for practical purposes). Fingerprints, iris patterns, and DNA profiles all satisfy both conditions to a degree that has been validated across decades of scientific study. Facial geometry and voiceprints are somewhat more variable, which is why they are typically used in combination with other identifiers rather than as standalone evidence.

In the criminalistics context specifically, biometrics serves three functions. The first is **scene-to-person linkage**—connecting physical evidence found at a crime scene to a specific individual (the classic fingerprint or DNA match). The second is **person-to-record linkage**—establishing that a person in custody or before a court is the same person recorded in a database (identity verification). The third is **cross-case linkage**—identifying connections between separate incidents through shared biological or

physical signatures (a serial offender whose DNA appears at multiple scenes, for example). Each function has its own procedural requirements, its own reliability profile, and its own legal implications.

What all three functions share is dependence on the quality and integrity of the underlying data. A biometric match is only as reliable as the sample collection process, the laboratory analysis, the database against which it is compared, and the chain of custody that connects the crime scene to the courtroom. Each of those steps is a potential point of failure, and Indian forensic infrastructure has well-documented weaknesses at several of them.⁹¹¹ Understanding biometrics in criminal investigation requires taking those weaknesses seriously, not treating the technology as infallible because it is scientific.

III. TYPES OF BIOMETRICS IN FORENSIC EVIDENCE

3.1 Fingerprints

Fingerprints remain the foundation of biometric evidence in Indian criminal proceedings, and their continued dominance reflects genuine reliability rather than mere institutional inertia. The ridge patterns of the fingertips are formed during foetal development, remain stable throughout life, and are sufficiently complex that the probability of two individuals sharing identical prints is, for practical purposes, vanishingly small. Latent prints—impressions left on surfaces through contact with sweat and oils—can be recovered from a crime scene and compared against a suspect's known prints or searched against a database through Automated Fingerprint Identification Systems (AFIS).

The legal framework for fingerprint evidence has been stable for decades. In *State of Maharashtra v. Suresh*,⁹¹² the Supreme Court confirmed the admissibility of fingerprint evidence and the weight to be accorded expert testimony on fingerprint matching under what was then

⁹¹¹National Accreditation Board for Testing and Calibration Laboratories (NABL), Accreditation of Forensic Laboratories: Policy Document (2021).

⁹¹²*State of Maharashtra v. Suresh*, (2000) 1 SCC 471 (India).

Section 45 of the Indian Evidence Act—now carried over into the BSA. The Court was equally clear, however, that fingerprint evidence is corroborative: it supports a prosecution case, it does not substitute for one. That qualification matters in practice, because the tendency to treat an AFIS match as conclusive—rather than as one element in a larger evidentiary picture requiring independent verification—remains a persistent problem in how this evidence is presented and received.

3.2 Iris and Retinal Scans

The iris—the pigmented ring surrounding the pupil—develops its unique pattern in the first year of life and remains essentially unchanged thereafter. Iris recognition systems photograph the iris, extract its distinctive features, convert them to a digital template, and compare that template against a reference database. The technique is considered among the most accurate available, with false match rates in controlled conditions measurable in parts per million. Retinal scanning examines the blood vessel pattern at the back of the eye and achieves similar accuracy, though it requires closer subject cooperation and more controlled conditions.

In India, iris scanning acquired mass-scale operational significance through Aadhaar,⁹¹³ where it is used alongside fingerprints to prevent duplicate enrolments across a database of over a billion records. In criminal investigation, iris-based identification is less frequently employed than fingerprinting, but its significance is growing as agencies with access to the Aadhaar database and the NCRB's biometric records begin using iris data to verify the identity of persons in custody or to link individuals to prior records.

3.3 Facial Recognition

Facial recognition technology works by mapping the spatial geometry of facial features—the distance between the eyes, the width of the nose,

the contour of the jaw—and matching that map against a reference database. Indian law enforcement agencies have deployed facial recognition in crowd surveillance at public events, identification from CCTV footage, and tracking of missing persons. The NCRB's Automated Facial Recognition System (AFRS) is among the largest databases of its type globally.

The technology is also the most scientifically contested of the major biometric modalities. Unlike fingerprints or iris patterns, facial geometry is affected by ageing, weight change, lighting conditions, image angle, and image quality. More significantly, multiple independent studies have documented systematic variation in accuracy by demographic group: error rates are measurably higher for women than for men, and higher for people with darker skin tones than for lighter-skinned subjects. The practical consequence is that the technology is least reliable for the groups least able to contest a false identification.

The legal vacuum around facial recognition deployment in India is a serious governance problem. Neither the BNSS nor any other current statute specifies the conditions under which law enforcement may use facial recognition, what accuracy thresholds must be met before a match can form the basis of an investigation, or what procedural protections apply when a match is used to justify an arrest or detention.⁹¹⁴ This is not a gap at the margins of the framework—it is the absence of a framework entirely for one of the most intrusive identification technologies the state has ever deployed.

3.4 DNA Profiling

DNA analysis identifies unique markers in the genetic code and compares them against a reference sample. Because every individual's genome is unique (with the narrow exception of identical twins), a match between evidentiary DNA and a reference sample is the most

⁹¹³Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, No. 18 of 2016 (India).

⁹¹⁴Telecom Regulatory Authority of India, Recommendations on Regulatory Framework for Artificial Intelligence & Machine Learning (2024).

definitive biological identification available to forensic science. It is also the most sensitive: a DNA profile discloses not merely who a person is but information about their health predispositions, ancestral origins, and biological relatives—none of whom consented to their genetic information being placed in a criminal database.

The evidentiary power of DNA profiling has been demonstrated in some of India's most significant cases. In the Nirbhaya gang rape and murder case,⁹¹⁵ DNA evidence was critical to establishing the identity of the accused and the sequence of events. In the Nithari serial murder investigation, DNA profiling identified victims from fragmented biological material that could not otherwise have been attributed. In *Santosh Kumar Singh v. State through CBI*,⁹¹⁶ the Supreme Court relied on DNA and forensic evidence in a conviction for murder and rape, affirming that properly conducted DNA analysis meets the standards of expert testimony under Indian evidence law.

The legal infrastructure for DNA evidence in India, however, remains incomplete. The DNA Technology (Use and Application) Regulation Bill was introduced in 2019 but has since lapsed without enactment,⁹¹⁷ leaving DNA banks, collection protocols, and permissible uses without dedicated statutory grounding. The BSA's general provisions on electronic and forensic evidence apply, but they were not designed with the specific sensitivities of genetic data in mind. The absence of a DNA regulation statute is not an abstract deficiency—it means there are no enforceable legal limits on what happens to a biological sample after the trial that generated its collection concludes.

3.5 Voice Recognition and Behavioural Biometrics

Behavioural biometrics capture individual-specific traits expressed through action: voice patterns, handwriting, gait, keystroke dynamics,

the rhythm of a signature. Voice recognition analyses acoustic properties—frequency, pitch, cadence—to create a voiceprint. These modalities are typically used as supplementary identifiers rather than primary evidence, given that behavioural traits are more susceptible to variation with circumstances than anatomical characteristics.

The Supreme Court's ruling in *Selvi v. State of Karnataka* is directly relevant here.⁹¹⁸ The Court held that techniques such as narcoanalysis, polygraph, and brain mapping—which compel the production of information through the analysis of involuntary physiological responses—violate Article 20(3)'s protection against self-incrimination. The ruling has implications for behavioural biometrics more broadly: where a technique involves compelled participation and extracts information of a testimonial character from the subject, the constitutional protection applies. Voluntary provision of a voice sample for comparison purposes stands on different footing from forced testing.

In *Ram Singh v. Sonia*,⁹¹⁹ the Supreme Court addressed handwriting comparison as a form of expert evidence, holding that it is admissible when conducted by a qualified expert but remains subject to the general requirements of reliability and corroboration. The evidentiary framework for other behavioural biometrics is less well developed, with courts applying the general expert testimony provisions of the BSA on a case-by-case basis.

IV. BIOMETRICS IN THE INVESTIGATIVE AND SCIENTIFIC PROCESS

4.1 Scene to Courtroom: The Forensic Chain

The integrity of biometric evidence in criminal proceedings depends on what happens at every stage between collection and courtroom presentation. A fingerprint or DNA match has no evidentiary value—indeed, it risks being dangerously misleading—if the sample was

⁹¹⁵Mukesh v. State for NCT of Delhi, (2017) 6 SCC 1 (India) (Nirbhaya gang rape case).

⁹¹⁶Santosh Kumar Singh v. State through CBI, (2010) 9 SCC 747 (India).

⁹¹⁷DNA Technology (Use and Application) Regulation Bill, 2019, Bill No. 15 of 2019 (India) (lapsed, Seventeenth Lok Sabha).

⁹¹⁸Selvi v. State of Karnataka, (2010) 7 SCC 263 (India).

⁹¹⁹Ram Singh v. Sonia, (2007) 3 SCC 1 (India).

contaminated at the scene, mishandled during transportation, or processed in an unaccredited laboratory. This is the chain-of-custody principle, and it underpins the BSA's certification requirement for electronic and forensic records.⁹²⁰

Indian forensic infrastructure has well-documented capacity constraints. There are relatively few accredited forensic science laboratories in proportion to the volume of criminal cases; case backlogs are extensive; and the standards of laboratory practice vary significantly across states and between metropolitan and district-level facilities. The National Forensic Science University Act, 2020 represents a policy commitment to building capacity,⁹²¹ and the CSIR network provides some national scientific infrastructure,⁹²² but the gap between the investigative aspiration and the forensic reality remains large in many parts of the country.

4.2 AFIS and Database-Driven Investigation

Automated Fingerprint Identification Systems work by converting a fingerprint image into a set of distinctive features—minutiae points where ridges end or bifurcate—and comparing those features against a database of stored templates. When a scene print is run against the database, the system returns a ranked list of candidate matches; the final identification decision is made by a trained examiner who compares the candidates against the original. The system is a search tool, not a decision-making one, and the examiner's judgment remains essential.

The NCRB operates the national AFIS and maintains the central database into which state-level records are aggregated. The CPI Act 2022 has significantly expanded the range of persons whose biometric data is added to this database—covering not just convicted persons

(as under the 1920 Act) but arrested persons and persons detained in connection with specified offences.⁹²³ The investigative benefit is real: a larger database means more potential matches. The rights implication is equally real: the biometric records of people who are arrested but not convicted—who may ultimately be found innocent—are nevertheless retained in the national database for extended periods.

4.3 DNA Databases and the Missing Statute

India's forensic DNA practice operates without the dedicated regulatory statute that would normally govern a national DNA database of the scale and sensitivity involved. The Directorate of Forensic Science Services has issued guidelines on DNA profiling,⁹²⁴ and the NABL accreditation framework applies to forensic laboratories, but these administrative instruments are not a substitute for primary legislation. They cannot create enforceable rights for data subjects, they cannot impose binding limits on retention or use, and they cannot be challenged in court in the same way that a statute can.

The DNA Technology Regulation Bill, which would have established a DNA Regulatory Board, governed the establishment of DNA data banks, and set rules for the collection, use, and deletion of DNA profiles, was introduced in 2019 and has since lapsed. Its absence is the single most significant legal gap in India's biometric evidence framework. Every other major jurisdiction with a national forensic DNA capability—the United Kingdom, the United States, Germany—has enacted primary legislation governing it. India has not, and the consequences are felt every time a biological sample is collected in a criminal investigation without any statutory guarantee of what becomes of it.

⁹²⁰Bharatiya Sakshya Adhiniyam, No. 47 of 2023, Sec 39 (India).

⁹²¹Ministry of Home Affairs, National Forensic Science University Act, No. 32 of 2020 (India).

⁹²²Council of Scientific and Industrial Research, Annual Report 2022–23 (2023).

⁹²³Criminal Procedure (Identification) Act, No. 11 of 2022, §§ 3–5 (India).

⁹²⁴Directorate of Forensic Science Services, Ministry of Home Affairs, Guidelines on DNA Profiling (2019).

4.4 Facial Recognition in Law Enforcement Practice

The practical deployment of facial recognition by Indian police forces has expanded substantially in recent years—at major public events, railway stations, airports, and as part of missing persons initiatives. The technology is powerful. It is also deployed without any statutory authorisation, without published accuracy standards, without an independent oversight mechanism, and without any procedural requirement that a match be corroborated before it is acted upon.

The European Union's General Data Protection Regulation treats biometric data used for identification as a special category requiring explicit statutory authorisation and heightened safeguards.⁹²⁵ India has no equivalent provision in the DPDPA 2023. The Telecom Regulatory Authority of India has begun to address the regulatory implications of artificial intelligence, but facial recognition law enforcement applications are not covered by the telecommunications framework. The result is a technology with enormous implications for civil liberties operating, in practice, on the basis of executive discretion alone.

V. PROBLEMS AND POLICY CHALLENGES

5.1 Privacy: The Irreversibility Problem

The fundamental privacy concern with biometric data is not simply that it is sensitive—so is medical data, financial data, and communications data. It is that it is irreversible. A compromised password can be reset. A breached biometric cannot. The fingerprints or iris patterns stored in a database are yours for life; if they are leaked or misused, there is no remediation that restores the uniqueness of your biological identifiers. This irreversibility changes the risk calculus for data protection in ways that the current legal framework does not fully reflect.

The *Puttaswamy* proportionality test requires that any state intrusion on privacy satisfy four conditions: legality (must be authorised by law), legitimate aim (must serve a genuine state interest), proportionality (must be no more intrusive than necessary), and procedural guarantees against abuse.⁹²⁶ Applied to biometric data collection in criminal investigations, the test raises real questions about several current practices. Collecting iris scans and DNA from persons who are arrested but ultimately acquitted may satisfy legality (the CPI Act authorises it) and legitimate aim (criminal investigation is a genuine state interest), but it is much harder to satisfy proportionality and procedural guarantees when the data is retained for decades after the person has been found innocent.

5.2 The Consent Fiction in Compelled Collection

The language of consent appears in India's biometric regulatory framework—the SPDI Rules require it, and the DPDPA 2023 makes it a central concept. But consent is a fiction when the state is doing the collecting. A person in custody instructed by police to submit to iris scanning or provide a DNA swab is not exercising a meaningful choice. The practical question is not whether they "consent" but whether the compelled collection is authorised by law and proportionate to the investigation—and whether there are adequate safeguards against the data being used for purposes beyond the investigation that justified its collection.

The SPDI Rules' exclusion of government agencies from their consent requirements is the most direct expression of this problem.⁹²⁷ The agency with the greatest power to compel biometric collection—the state—is also the agency with the least legal constraint on how it does so. The CPI Act 2022 has expanded collection powers without adding proportionality safeguards, purpose limitation principles, or

⁹²⁵General Data Protection Regulation, Regulation 2016/679 of the European Parliament and of the Council, art. 9 (2016).

⁹²⁶K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, ¶ 309 (India) (Chandrachud, J., concurring).

⁹²⁷Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 3, G.S.R. 313(E) (India).

independent oversight mechanisms that would give the affected person any practical recourse.

5.3 The Law Has Not Kept Up

India has built biometric infrastructure at a pace that outstrips its legal development. Aadhaar enrolled a billion people before there was a data protection law. Facial recognition systems were deployed at scale before any statute authorised them. The DNA database is growing without a DNA regulation statute. The CPI Act expanded collection powers without incorporating the proportionality principles the courts had already identified as constitutionally required. The DPDPA 2023, when it finally arrived, created a framework that treats biometric data as ordinary personal data and exempts the state from significant obligations.⁹²⁸

This is not the story of technology moving faster than law everywhere—it is a story of specific legislative choices (or non-choices) that have left rights-protective frameworks underdeveloped. The gap matters in concrete terms: without statutory retention limits, biometric data persists indefinitely. Without purpose limitation, it can be repurposed freely. Without independent oversight, there is no systematic check on agency compliance with the procedural requirements that do exist.

5.4 Mission Creep and the Aadhaar Model

Aadhaar began as a welfare delivery mechanism and has since become a de facto prerequisite for banking, mobile communications, income tax, and a wide range of private services. This expansion happened incrementally, through executive decisions rather than comprehensive parliamentary deliberation. The Supreme Court in *Puttaswamy* drew the line at mandatory private sector linkage, holding it disproportionate, but the broader phenomenon—of data collected for one purpose being steadily repurposed for others—remains structurally embedded in how India has built its biometric architecture.

For law enforcement biometrics specifically, mission creep takes the form of investigative databases being used for purposes beyond criminal investigation—immigration enforcement, general surveillance, identity verification for services unrelated to the offence that justified the original collection. The CPI Act does not contain a purpose limitation clause that would prevent this. The DPDPA's state entity exemptions would not catch it. The constitutional proportionality standard in *Puttaswamy* provides the only meaningful check, and it operates only when someone has both the knowledge that their data is being misused and the resources to litigate.

5.5 Infrastructure, Accuracy, and Inequality

Advanced biometric systems are only as good as the infrastructure that runs them. AFIS, DNA analysis, and facial recognition all require expensive equipment, trained personnel, controlled environments, and quality assurance processes. These resources are not evenly distributed across India. A forensic laboratory in Mumbai or Delhi operates under conditions that are simply unavailable to a district-level facility in a more remote state. The reliability of biometric evidence therefore varies with geography in ways that the legal framework does not acknowledge or compensate for.

Courts applying the BSA's certification requirement for electronic records do not typically have access to information about the accreditation status of the laboratory that generated the biometric evidence, the error rate of the specific AFIS system used, or the quality score of the fingerprint or DNA sample on which the match was based. Expert witnesses are not uniformly required to disclose these figures. The result is that courts may place weight on biometric evidence that does not, in the specific instance, merit it—and the people most likely to bear the consequences are those with the least ability to mount an effective challenge.

⁹²⁸Digital Personal Data Protection Act, No. 22 of 2023 (India).

5.6 Marginalised Communities and the Surveillance Risk

The disproportionate impact of biometric surveillance on marginalised communities is not a hypothetical concern. Facial recognition systems show higher error rates for women and people with darker skin tones—the same communities that are already subject to elevated levels of policing. A system that is least accurate for the groups most intensively surveilled does not merely risk individual wrongful identifications; it structurally embeds pre-existing discrimination into the criminal justice process.⁹²⁹

The expansion of the criminal biometric database under the CPI Act to cover arrested persons (not just convicts) compounds this problem. If certain communities are disproportionately arrested—whether through targeted policing or structural disadvantage—their biometric data will be disproportionately represented in the database, generating more matches, which can generate more investigations and more arrests in a self-reinforcing cycle. This is not a risk that any existing statute is designed to detect, monitor, or prevent.

VI. INDIA'S LEGAL FRAMEWORK FOR BIOMETRICS

6.1 The Identification of Prisoners Act, 1920 and Its Replacement

The Identification of Prisoners Act, 1920 was India's first statutory framework for the collection of physical measurements from persons in custody.⁹³⁰ It authorised the taking of fingerprints and footprints from convicted persons and, in limited circumstances, from persons arrested for certain offences. For over a century, this narrow framework governed what the state could collect. The Criminal Procedure (Identification) Act, 2022 replaced it with something substantially more expansive: a regime that covers iris scans, blood samples, biological samples, and behavioural measurements,

collected from a broader range of persons, stored in a centralised national database, and retained for extended periods. The transition represents a fundamental shift in the state's biometric capabilities—one that deserves more careful legal scrutiny than it has received.

6.2 The SPDI Rules, 2011

The Information Technology (Sensitive Personal Data or Information) Rules, 2011 were the first piece of Indian law to recognise biometric data as a category deserving heightened protection. They required explicit written consent, purpose limitation, and reasonable security practices from private body corporates handling biometric information. The framework was a meaningful step forward in the private sector context. Its limitation is definitional: "body corporate" excludes government agencies. The most powerful collectors of biometric data in India—police, immigration authorities, welfare administrators—operate outside these rules entirely.

6.3 The Aadhaar Act, 2016

The Aadhaar Act provides the statutory foundation for the world's largest biometric identity system. It includes security obligations, restricts sharing of core biometric data, and created the Unique Identification Authority of India as the governing body. What it did not do—and could not have done, since the constitutional framework came a year later—was incorporate the proportionality and procedural guarantee standards that *Puttaswamy* would establish. The Supreme Court's 2018 ruling on the Aadhaar Act upheld the core identity system but struck down mandatory private sector linkage as disproportionate, establishing that constitutional validity requires ongoing justification, not just initial legislative authorisation.

6.4 The Bharatiya Sakshya Adhiniyam, 2023

The BSA modernised the evidence framework, replacing the Indian Evidence Act 1872 and

⁹²⁹Amnesty International India, *Halt the Hate: Crimes Against Dalits in India* (2023).

⁹³⁰Identification of Prisoners Act, No. 33 of 1920 (India) (repealed 2022).

explicitly incorporating electronic records—including biometric data in digital form—as admissible evidence. Section 39 requires a certificate from a responsible official confirming the conditions of production and a hash value demonstrating data integrity. This is the most practically significant evidentiary safeguard in the current framework: a court now has a formal basis for excluding biometric evidence where its integrity is not certified, and defence counsel has a defined point of challenge.

The limitation of Section 39 is that it addresses integrity, not reliability. A perfectly certified AFIS match is certified only to be what it purports to be—the output of a particular system operating on a particular sample. Whether the system is accurate enough for the purpose, whether the sample was sufficient quality, whether the examiner's conclusions are methodologically sound: none of these questions are answered by the certificate. Courts applying Section 39 will need to continue asking the foundational questions about scientific methodology that belong in any rigorous assessment of expert evidence.

6.5 The Digital Personal Data Protection Act, 2023

The DPDPA 2023 arrived as the long-awaited comprehensive data protection statute. For biometrics specifically, it is disappointing in two respects. First, unlike the GDPR, which treats biometric data used for identification as a special category with a higher protection threshold, the DPDPA does not distinguish biometric data from other personal data. All personal data is subject to the same framework, regardless of its irreversibility, its sensitivity, or its potential for misuse. Second, the state entity exemptions are wide. The government can invoke "legitimate uses" in ways that bypass consent requirements; security agencies are explicitly excluded from significant obligations. The law that was meant to provide the backstop for biometric data protection has left the most

powerful actors in the biometric ecosystem largely unregulated.

6.6 The Criminal Procedure (Identification) Act, 2022

The CPI Act 2022 is the statute that most directly governs biometric collection in the criminal justice context. It authorises police to collect fingerprints, palm prints, footprints, photographs, iris scans, blood samples, and other biological samples from convicted persons, arrested persons, and persons detained in connection with specified offences. Measurements are to be forwarded to the NCRB for the national database and may be retained for up to seventy-five years. A magistrate may authorise collection from persons not otherwise covered, on police application.

The Act has been challenged on constitutional grounds in multiple High Courts, with the central question being whether extended retention of biometric data from persons who are ultimately acquitted satisfies the proportionality standard in *Puttaswamy*. *Paramvir Singh Saini v. Baljit Singh* had already indicated that indefinite retention could not be sustained.⁹³¹ The CPI Act's response—periods of up to seventy-five years with provisions for deletion on acquittal that are discretionary rather than automatic—is unlikely to fully satisfy the proportionality analysis.⁹³² The absence of a built-in purpose limitation principle, independent oversight mechanism, or right to know that one's data is being retained compounds the constitutional concern.

VII. LAW COMMISSION REPORTS ON BIOMETRICS IN CRIMINAL JUSTICE

The Law Commission of India has addressed biometric evidence and forensic science in several reports spanning four decades, with each report reflecting both the technology and the legal thinking of its time.

⁹³¹*Paramvir Singh Saini v. Baljit Singh*, (2021) 11 SCC 129 (India).

⁹³²Rajya Sabha Debates, Statement of Objects and Reasons, Criminal Procedure (Identification) Bill, 2022 (Apr. 4, 2022).

7.1 The 18th Report (1980)

The 18th Report, which reviewed the Indian Evidence Act, addressed forensic science methodology and recommended standardisation of fingerprint and other physical evidence protocols across the country's forensic laboratories.⁹³³ At the time, DNA profiling had not yet entered forensic practice, and the Report's focus was principally on fingerprinting, handwriting comparison, and the qualifications of expert witnesses. Its recommendations fed into the eventual development of the Central Forensic Science Laboratory network, though the gap between recommendation and comprehensive implementation remains visible to this day. The Report's call for standardised protocols and accredited laboratories was prescient; the failure to fully implement it has contributed to the quality disparities that still affect biometric evidence in Indian courts.

7.2 The 262nd Report on the Death Penalty (2015)

The 262nd Report addressed the use of forensic evidence—including biometric and DNA evidence—in capital cases.⁹³⁴ The Commission's concern was straightforward: the irreversibility of a death sentence demands a higher standard of evidentiary reliability than ordinary criminal conviction. Where biometric evidence is used to support a capital charge, the procedures for collection, analysis, and presentation must be robust enough to exclude the possibility of error at an acceptable level of confidence. The Report called for enhanced procedural safeguards against tampering, greater transparency about the methodology and limitations of forensic analysis, and more rigorous scrutiny of expert witness qualifications.

The Report also noted the risk of courts placing undue weight on forensic evidence simply because it is scientific. A DNA match or fingerprint identification can be wrong—through contamination, laboratory error, or deliberate

tampering—and the scientific framing of such evidence can make it disproportionately persuasive to judges and juries who lack the expertise to assess its reliability independently. The Commission's call for greater judicial education on forensic science methodology remains relevant and has not been fully acted upon.

7.3 The 277th Report on Witness Protection (2018)

The 277th Report, addressing witness identity protection and witness protection programmes, engaged with biometric data in the context of identity security for protected witnesses.⁹³⁵ The Report was not primarily a forensic evidence document, but its analysis of the risks created by inadequate biometric data security—and the consequences for individuals who depend on the state's ability to protect their identities—speaks directly to broader themes in this paper. When biometric data held by state agencies is inadequately secured, the harm falls not just on the individual whose data is compromised but on the integrity of the entire process that depends on that data's confidentiality.

Across all three reports, a consistent theme emerges: the Commission has identified the value of biometric evidence while calling for the legal and institutional safeguards that would make its use reliable and accountable. The gap between what the Commission has recommended and what Parliament has enacted is itself a significant policy observation. Independent audit mechanisms for forensic laboratories, statutory DNA regulation, and enforceable data protection standards for criminal biometric databases have all been anticipated in Commission reports—and have all been slow to materialise in legislation.

VIII. CASE LAW ON BIOMETRIC EVIDENCE

Indian courts have engaged with biometric evidence across a body of case law that reflects

⁹³³Law Commission of India, Report No. 18: Review of the Indian Evidence Act, 1872 (1980).

⁹³⁴Law Commission of India, Report No. 262: The Death Penalty (2015).

⁹³⁵Law Commission of India, Report No. 277: Witness Identity Protection and Witness Protection Programmes (2018).

a consistent tension: recognition of its forensic value alongside real concern about the risks of over-reliance, constitutional overreach, and the absence of adequate procedural safeguards. The trajectory of the case law is broadly from establishing admissibility to scrutinising proportionality—a progression that mirrors the increasing power and intrusiveness of the technology itself.

State of Maharashtra v. Suresh (2000)

In *State of Maharashtra v. Suresh*, the Supreme Court affirmed the admissibility of fingerprint evidence and gave substantial weight to expert testimony on fingerprint matching under Section 45 of the Indian Evidence Act. At the same time, the Court was explicit that fingerprint evidence is corroborative in character—it strengthens a prosecution case but does not substitute for one. A conviction cannot rest on fingerprint evidence alone without additional evidence establishing the accused's guilt. This proportionate approach has remained the baseline for fingerprint evidence and has been implicitly adopted in relation to other biometric modalities under the BSA.

Selvi v. State of Karnataka (2010)

In *Selvi v. State of Karnataka* the Supreme Court held that narcoanalysis, polygraph testing, and brain mapping conducted without the subject's consent violate Article 20(3)'s right against self-incrimination and Article 21's right to life and personal liberty. The ruling established that techniques which compel the disclosure of information by measuring involuntary physiological responses—whether or not their outputs are technically biometric—cannot be used as evidence when administered without consent. The ruling is directly relevant to any biometric technique that involves compelled participation and extracts information of a testimonial character.

Santosh Kumar Singh v. State through CBI (2010)

In *Santosh Kumar Singh v. State through CBI*, the Supreme Court upheld a murder and rape conviction in which forensic and DNA evidence played a central role, affirming that properly conducted DNA analysis constitutes admissible expert evidence under the Indian evidence framework. The case established that the scientific validity of DNA profiling is beyond doubt—the question for courts is not whether the technique is reliable in principle but whether the specific analysis was conducted in accordance with appropriate protocols and by a qualified expert. It set the template for how courts should approach DNA evidence: accepting its scientific basis while maintaining rigorous scrutiny of its specific application.

Mukesh v. State for NCT of Delhi (2017)

In *Mukesh v. State for NCT of Delhi* (the Nirbhaya case), the Supreme Court confirmed convictions supported by a substantial body of forensic evidence including DNA profiling, forensic pathology, and electronic evidence. The case demonstrated the cumulative power of biometric and scientific evidence when it is collected, analysed, and presented in accordance with proper procedure. It also illustrated the BSA's predecessor's framework for electronic evidence, anticipating the certification and integrity requirements that the BSA now makes explicit.

Shafhi Mohammad v. State of Himachal Pradesh (2018)

In *Shafhi Mohammad v. State of Himachal Pradesh*,⁹³⁶ the Supreme Court addressed the admissibility of video recordings and electronically stored biometric identification evidence in police investigations. The Court held that such evidence is admissible but that its collection must observe privacy safeguards consistent with Article 21. This was a significant development: it moved the constitutional inquiry beyond the question of admissibility to the

⁹³⁶*Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801 (India).

manner of collection, establishing that the means by which biometric evidence is gathered affects its constitutional validity, not merely its technical reliability.

Justice K.S. Puttaswamy v. Union of India (2017)

The *Puttaswamy* nine-judge bench ruling is the constitutional lodestar for all biometric law and policy in India. The Court's unanimous recognition of privacy as a fundamental right under Article 21 established that any state action involving the collection, processing, or use of personal data—including biometric data—must satisfy the four-fold test of legality, legitimate aim, proportionality, and procedural guarantees. For criminal justice biometrics specifically, this means that police powers to collect and retain biometric data must be grounded in statute, must serve a genuine investigative purpose, must be no more intrusive than necessary to achieve that purpose, and must be accompanied by meaningful safeguards against misuse. Whether the current statutory framework—particularly the CPI Act 2022—satisfies these conditions is the central constitutional question in this area.

Paramvir Singh Saini v. Baljit Singh (2021)

In *Paramvir Singh Saini v. Baljit Singh*, the Supreme Court scrutinised the data retention aspects of the criminal identification framework and held that indefinite retention of biometric data from persons who have been acquitted is constitutionally unsustainable. The ruling sent a clear signal: the state's power to collect biometric data in the course of a criminal investigation does not carry with it an unlimited power to retain it. The data collected must serve the investigation that justified its collection; once that purpose has been exhausted—as it is when an acquittal ends the criminal proceedings—the continued retention of the data requires fresh justification.

IX. RELEVANT PROVISIONS IN BNS, BNSS, AND BSA

9.1 Bharatiya Nyaya Sanhita, 2023

Section 53 of the BNS empowers a magistrate to order a medical examination of an arrested person where it is material to the investigation of a serious offence.⁹³⁷ The new framework has expanded the scope of that examination to include biometric data collection—DNA samples, iris scans, and biological samples—beyond what was permissible under the corresponding provision of the Code of Criminal Procedure. The provision is framed principally around investigative utility; it does not include an explicit proportionality requirement, a defined threshold of offence seriousness below which biometric collection is impermissible, or any right for the person to contest the order before collection takes place.

Read against the *Puttaswamy* standard, the absence of a proportionality safeguard in Section 53 is a textual gap with constitutional implications. A magistrate directing biometric collection under this section is exercising a power that, under the constitutional framework, must be proportionate to the investigative need. The section would benefit from an explicit requirement that the magistrate be satisfied that the collection is necessary and proportionate before issuing the order.

9.2 Bharatiya Nagarik Suraksha Sanhita, 2023

Section 54A of the BNSS authorises police to take biometric measurements—fingerprints, iris scans, blood samples, and other measurements specified by the Central Government—from arrested persons.⁹³⁸ The data collected is to be forwarded to the NCRB for inclusion in the central database maintained under the CPI Act. Section 185 of the BNSS facilitates the submission of digital evidence, including biometric logs and electronic records, in proceedings before courts and magistrates. Together, Sections 54A and 185 create the procedural pipeline through which

⁹³⁷Bharatiya Nyaya Sanhita, No. 45 of 2023, § 53 (India).

⁹³⁸Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, §§ 54A, 185 (India).

biometric data moves from the investigation to the evidentiary record.

Two features of Section 54A are notable for a rights analysis. First, the section authorises collection from anyone who has been arrested—not just persons charged with or convicted of serious offences. Second, there is no purpose limitation clause: data collected in connection with one offence can, under the current framework, be retained in the national database and potentially used in entirely unrelated future investigations. The *Puttaswamy* proportionality analysis requires that collection be tied to a specific legitimate purpose; Section 54A as drafted does not make that connection explicit.

9.3 Bharatiya Sakshya Adhiniyam, 2023

Section 39 of the BSA defines electronic records broadly enough to encompass biometric data in digital form—fingerprint templates, iris scan records, DNA profiles stored electronically—and declares them admissible in evidence, subject to the certification and hash value requirements already discussed. The provision reflects a deliberate policy decision to place electronic and digital forensic evidence on the same footing as paper documents, recognising that modern criminal investigations generate primarily digital evidentiary records.

The section's most important contribution is the certification requirement. By making admissibility conditional on a responsible official certifying the conditions of production and a hash value confirming data integrity, Section 39 creates a formal procedural checkpoint that did not exist under the old framework. A certificate is challengeable; its absence is a defined ground for exclusion; its presence at least establishes a minimum standard of documentary chain of custody. This matters enormously for biometric evidence, where the risk of contamination, tampering, or database error is real and must be subject to some form of verification.

What Section 39 does not provide is an answer to questions of scientific reliability. The section's certification requirement establishes that the

data is what it purports to be—it does not establish that the methodology that generated the data is valid, that the expert who interpreted it is qualified, or that the margin of error is acceptable for the purpose. Courts applying the BSA will need to continue asking those questions independently, ideally with the assistance of the kind of forensic expert evidence that Section 39 implicitly contemplates.

X. COMPARATIVE PERSPECTIVES AND POLICY RECOMMENDATIONS

10.1 What Other Jurisdictions Have Done

The challenge of regulating biometric technology in criminal justice is not unique to India, and the approaches taken by other jurisdictions offer useful reference points—not as models to be copied wholesale but as illustrations of the range of solutions available.

The European Union's GDPR treats biometric data used for identification as a special category of personal data, requiring explicit statutory authorisation and heightened safeguards before processing. The AI Act, which entered into force in 2024, restricts the use of real-time facial recognition in public spaces by law enforcement to a closed list of serious offences with prior judicial authorisation. The United Kingdom's National DNA Database operates under the Police and Criminal Evidence Act and accompanying codes of practice, with defined retention periods, deletion requirements on acquittal, and oversight by a statutory ethics group. The United States operates through a patchwork of federal and state legislation, but the FBI's CODIS DNA database has specific statutory authorisation, profiling standards, and destruction requirements.

None of these frameworks is perfect, and each reflects the specific legal and political context in which it was developed. But all of them share features that India's current framework lacks: statutory authorisation for specific technologies (not just for biometrics in general), independent oversight bodies, explicit retention limits tied to

the purpose of collection, and deletion requirements when that purpose is exhausted.

10.2 What India Needs

The reforms most urgently needed in India's biometric law and policy framework can be organised around four themes.

First, **a dedicated DNA regulation statute**. The DNA Technology Regulation Bill should be reintroduced and enacted. It should establish a statutory DNA Regulatory Board, define the categories of offences for which DNA collection is permissible, specify mandatory accreditation requirements for laboratories, set enforceable retention limits with automatic deletion on acquittal, and create rights of access and correction for data subjects.

Second, **statutory authorisation for facial recognition**. The deployment of facial recognition by law enforcement should not continue on the basis of executive discretion alone. Parliament should enact primary legislation specifying the purposes for which facial recognition may be used, the accuracy thresholds it must meet, the judicial or quasi-judicial authorisation required before it is deployed in a specific investigation, and the procedural rights of persons identified through its use.

Third, **reform of the CPI Act's retention provisions**. The Act's retention periods should be amended to require automatic deletion of biometric data from persons who are acquitted, bringing the statute into line with the proportionality standard that *Paramvir Singh Saini* and *Puttaswamy* require. A purpose limitation clause should be added to prevent data collected in connection with one investigation from being used in unrelated proceedings without fresh authorisation.

Fourth, **biometric-specific protections in the DPDPA**. The Act should be amended to recognise biometric data as a special category, as the GDPR does, with a higher protection threshold that applies to state actors as well as private ones. The state entity exemptions should be

narrowed so that the agencies with the greatest biometric collection powers are subject to the most rigorous data protection obligations, not the most permissive ones.

XI. CONCLUSION

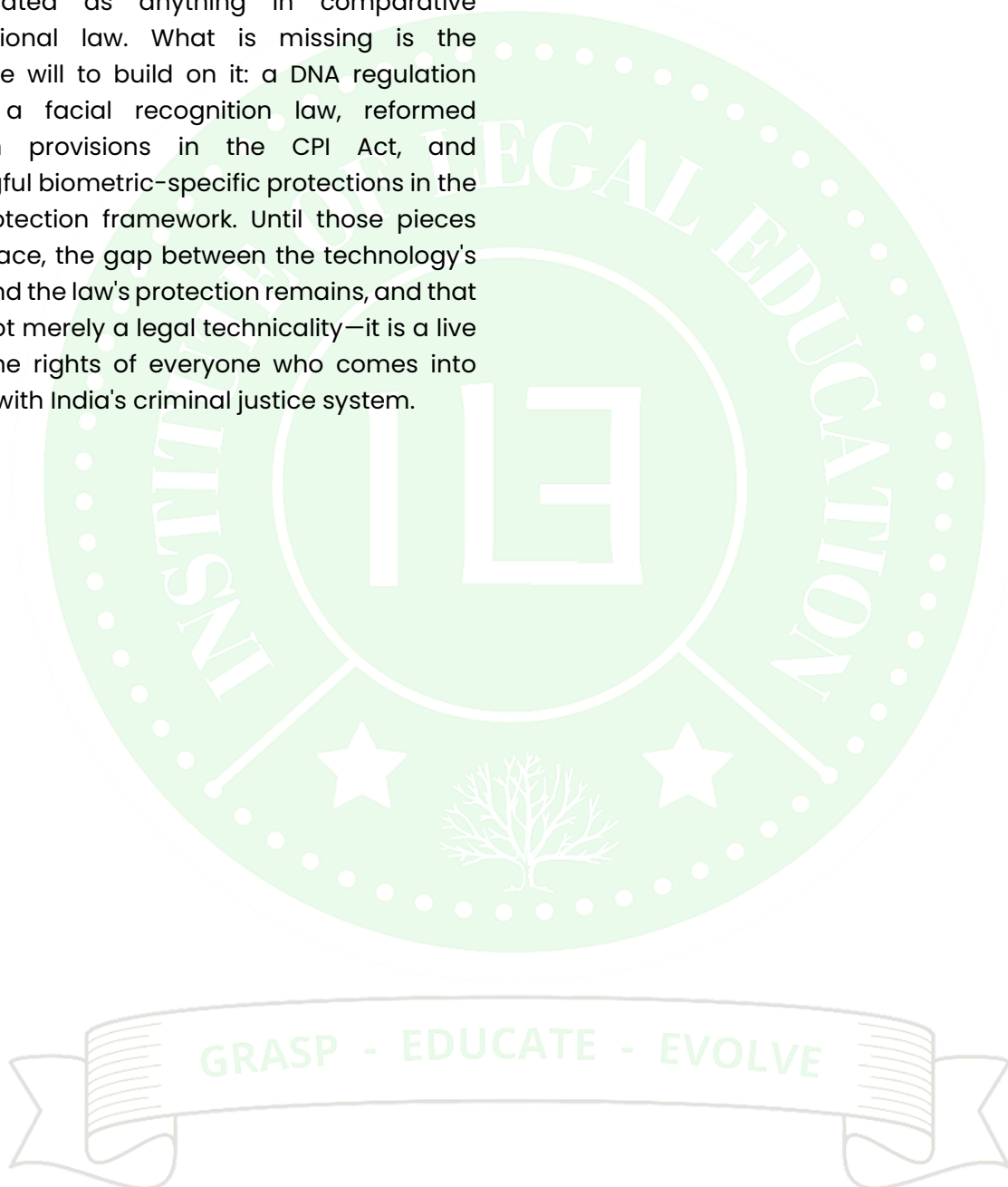
Biometric technology has genuinely transformed what is possible in Indian criminal investigation and forensic science. The fingerprint that solves a cold case, the DNA profile that identifies a victim's remains, the iris scan that catches a fraudulent welfare claim—these are not hypothetical benefits. They are real, and they represent a meaningful contribution to the quality and accuracy of criminal justice outcomes. The question is not whether to use biometrics. The question is whether the legal framework within which they are used is adequate to the task of ensuring that their power is exercised accountably and within constitutional limits.

The honest answer is that it is not—not yet. India has built biometric infrastructure of extraordinary scale and ambition without the legal architecture that should accompany it. The DNA database grows without a DNA regulation statute. Facial recognition is deployed across the country without statutory authorisation. The CPI Act expands collection powers without incorporating the proportionality safeguards that *Puttaswamy* demands. The DPDPA arrived too late and with too many state exemptions to fill the gap. The new criminal law statutes—BNS, BNSS, BSA—modernise the procedural framework in important ways, but they do not resolve the underlying policy question of how biometric data should be governed in a constitutional democracy.

The courts have done their part. *Puttaswamy* established the constitutional standard. *Selvi* protected against compelled self-incrimination through biometric testing. *Paramvir Singh Saini* drew the line at indefinite retention of acquitted persons' data. Judicial scrutiny is a necessary check, but it is a correction mechanism—it operates after the harm has already occurred and only when a litigant with resources chooses

to contest. Legislation that prevents the harm from occurring in the first place is a better answer than litigation that corrects it after the fact.

India has the constitutional foundations for a world-class biometric governance framework. The *Puttaswamy* proportionality standard is as sophisticated as anything in comparative constitutional law. What is missing is the legislative will to build on it: a DNA regulation statute, a facial recognition law, reformed retention provisions in the CPI Act, and meaningful biometric-specific protections in the data protection framework. Until those pieces are in place, the gap between the technology's power and the law's protection remains, and that gap is not merely a legal technicality—it is a live risk to the rights of everyone who comes into contact with India's criminal justice system.





INSTITUTE OF LEGAL EDUCATION

(Managed by L TO J LAW ASSOCIATES)

NO. 08, ARUL NAGAR, SEERA THOPPU,
MARUDHAANDA KURICHI, SRIRANGAM - 620102,
TAMILNADU, INDIA.

ISSN 2583-2344



9 772583 234004