Page 890 - 907 **DOI:** *https://doij.org/10.10000/IJLMH.1111250*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 1

2026

From Fingerprints to Facial Recognition: Constitutional Implications of Technological Expansion under Criminal Procedure (Identification) Act, 2022

RAHAMATHULLA S[1] AND DR. M.A. SALEEM AHMED[2]

ABSTRACT

In the digitalization era, unrestricted information is circulated around the universe if the progress of the technology and the monitoring methodology of the government. It is the equilibrium between the individual life, liberty, privacy and protection and security of the nation with evolving tension in the society. In the earlier stages the Identification of Prisoners Act was implemented to identify the criminals from measurements that had been taken from the accused. The surveillance of the accused person is controversial over the balance between privacy and security during the criminal justice system. Through the emerging techniques of the criminal identification methods and forensic science by the use of DNA testing, polygraphy, Narco analysis, Brain Electrical Actuating Profiling (BEAP) profiling, etc. The new technology involves carrying out fair investigations and ensuring proper prosecution during the criminal justice delivery system. In the early stages, they mostly depend upon the "eyewitnesses" but it is difficult to prove very effective, as are more often the digital aids. The "third degree methods" for interrogation of the suspects in order to bring out the truth instead of using technological advancement. The rights to privacy are the basic principle of the democratic country to safeguard every individual from unjustified interference and uphold the integrity of the personal boundaries under the CPI Act. The measurements include the footprints, fingerprints, photo, iris and retinal scans, and behaviour and attitude of the accused person. It allows processing, storage, reservation and distribution and the deletion of the measurements for investigation and prevention of crime. This paper argues that the implementation of emerging technologies bolsters human rights and upholds constitutional values. The adoption of such technology is in line with the constitutional test of proportionality and does not violate the right to privacy and other individual rights.

Keywords: *Emerging Technology, Criminal Profiling, Privacy, Human Rights*

[1] Author is a Research Scholar at Crescent School of Law, B.S Abdur Rahman Crescent Institute of Science and Technology, Tamil Nadu, India.

[2] Author is an Associate Professor at Crescent School of Law, B.S Abdur Rahman Crescent Institute of Science and Technology, Tamil Nadu, India.

 [ISSN 2581-5369]

I. INTRODUCTION

On average 7,50,000 cases have been closed by the police every year in the last five years due to lack of evidence. Next-generation crimes cannot be tackled with old techniques and that the criminal justice system must be brought "to the next era". For over a century, India relied on the antiquated **Identification of Prisoners Act, 1920** a law severely limited in scope and utterly inadequate for prosecuting crimes in the digital age. This historical deficit often translated into procedural delays, reliance on outdated methods, and consequently, challenges in achieving high conviction rates, underscoring the urgent need for comprehensive legal reform. The enactment of the **Criminal Procedure (Identification) Act, 2022 (CPIA)** marks a watershed moment in India's journey toward a technologically advanced and more efficient criminal justice ecosystem. By introducing advanced tools such as biometrics, behavioural analysis, DNA profiling, and digital storage through the National Crime Records Bureau (NCRB), the Act represents a decisive move towards data-driven policing. However, this transformation also raises critical constitutional questions regarding privacy, bodily integrity, and the permissible limits of State surveillance in a democratic society. This paper argues that the CPIA 2022 represents a constitutionally valid, technologically advanced, and human-rights–aligned reform that strengthens India's crime-prevention architecture while respecting fundamental rights.

II. MAJOR LOOPHOLES IN IDENTIFICATION OF PRISONERS ACT, 1920

The Act was enacted during the colonial period and remain largely unchanged for over 102 years. Several structural, technological, and constitutional limitations made it obsolete. One of the major shortcomings was its extremely restricted understanding of "measurements" under section 3 and 4. The law permitted only the taking of fingerprints, footprints, and basic photographs, which made it unsuitable for using advanced forensic tools such as DNA profiling, iris scans, and other biometric or behavioural identifiers that form the backbone of contemporary scientific policing. Additionally, the 1920 framework provided no guidance on data retention, deletion, security, or access controls. With no safeguards for privacy or misuse, the Act became incompatible with constitutional standards recognised after the Supreme Court declared privacy a fundamental right in K.S. Puttaswamy v. Union of India[3]. The Act also failed to align with modern criminal-procedure and evidence requirements. These limitations collectively made the Identification of Prisoners Act, 1920 unsuited for present-day policing, ultimately prompting the introduction of the Criminal Procedure (Identification) Act, 2022.

[3] AIR 2018 SC (SUPP) 1841, 2019 (1) SCC 1, (2018) 12 SCALE 1

 [ISSN 2581-5369]

III. Need for the Criminal Procedure Identification Act 2022

In 1980, the Law Commission of India, in its 87th Report, reviewed the legislation and proposed several amendments. This review followed the Supreme Court's observations in State of U.P. v. Ram Babu Misra, which underscored the need for statutory revision. The Commission first recommended expanding the definition of "measurements" to include palm impressions, signature or handwriting samples, and voice specimens. It further advised permitting the collection of such measurements for proceedings beyond those under the Code of Criminal Procedure (CrPC). The Report also noted that the necessity for reform was evident from the numerous State-level amendments. Given advancements in forensic science, the Commission stressed the importance of recognising a wider range of measurements to support modern investigative requirements. The Expert Committee on Criminal Justice Reforms, headed by Dr. Justice V.S. Malimath, suggested in March 2003 that the 1920 Act should be revised to allow Magistrates to authorise obtaining DNA-related materials such as blood, hair, saliva, and semen. The Identification of Prisoners Act, 1920 designed for an era of conventional physical crimes has led to a persistent "evidence deficit" in modern investigations[4]. NCRB statistics show that conviction rates for IPC offences have fallen to around 57% in recent years, largely due to the lack of reliable evidence. Courts frequently record acquittals because cases depend on eyewitnesses, many of whom later turn hostile, rather than on objective scientific proof. This gap is stark in cybercrimes, where conviction rates remain as low as 1.6%–2%. Since the 1920 Act allowed only fingerprint collection, it left investigators unequipped to gather voice samples, iris scans, or other advanced biometrics required to trace technologically sophisticated offenders. By restricting the use of biological samples such as DNA and prohibiting modern biometric techniques, the old law compelled police to rely on vulnerable human testimony. The Criminal Procedure Identification Act, 2022 seeks to shift from "hostile witnesses" to "silent witnesses" by empowering investigators to collect scientific evidence that is objective, tamper-proof, and resistant to intimidation.

IV. Comparative analysis between identification of prisoners act 1920 and criminal procedure identification act 2022 emerging technologies in criminal justice: how india is adopting them

[4] Avatar singh vs State of Haryana 2006 CriLJ 1866

 [ISSN 2581-5369]

Basis of Comparison	Identification of Prisoners Act, 1920	Criminal Procedure (Identification) Act, 2022
Purpose of the Act	Enacted to assist colonial police in identifying convicts and certain offenders using basic physical measurements.	Introduced to modernise criminal investigation by enabling scientific, technology-driven identification and data management.
Definition of "Measurements"	Very narrow limited to fingerprints, footprints, and simple photographs.	Highly expanded includes fingerprints, palm prints, footprints, photographs, iris scans, retina, biological samples, behavioural attributes, and other modern biometrics.
Persons from whom data can be collected	Only convicted persons, persons arrested for selected offences, and detainees under certain conditions.	Any person arrested for any offence, convicted persons, persons detained under preventive laws, and even persons ordered by a Magistrate much wider scope.
Technological Integration	Designed in a pre-digital era no provision for electronic storage, database integration, or scientific tools.	Fully technology-enabled; data stored digitally by NCRB, integrated with national crime databases and digital forensic systems.
Role of NCRB	No national-level data-management agency involved; records maintained manually by local authorities.	NCRB empowered to collect, store, process, share, and delete data across all States and UTs through a centralised system.
Retention of Data	No clarity on retention, deletion, or time limits.	Data retained for 75 years unless deletion is allowed under specific conditions.
Privacy and Data-Protection Safeguards	No privacy safeguards drafted long before	Provides a structured framework, but still debated for adequacy; expected to operate within the

	constitutional recognition of right to privacy.	constitutional limits set by Puttaswamy.
Authority to Direct Collection	Primarily police officers and certain Magistrates; limited discretionary power.	Police officers up to the rank of Head Constable, prison officials, and Magistrates have expanded authority.
Use of Force	Ambiguous provisions regarding compulsion, leading to inconsistent practices.	Clearly states that persons may be required to allow measurements subject to legal procedures (though this also raises constitutional concerns).
Scope for Modern Forensics	Could not support DNA profiling, digital biometrics, or scientific analysis.	Designed for integration with medico-legal procedures, DNA analysis, and forensic technologies.
Relevance to Present-Day Crime	Outdated for cybercrime, organised crime, and technologically advanced offences.	Aligns with current policing needs, including AI-assisted identification, digital forensics, and predictive policing tools.
Legislative Intent	Colonial surveillance-oriented; meant to monitor "habitual offenders.	Focused on scientific policing, national security, and efficient criminal justice administration.

V. MODERNISATION OF INVESTIGATION METHOD

The 2022 Act expands the term "measurements" to include advanced biometrics and biological samples, which is a crucial step for utilizing cutting-edge forensic science. Inclusions Finger, impressions, palm-print impressions, footprint impressions, photographs, iris and retina scans, physical and biological samples and their analysis (e.g., DNA profiling), and behavioural attributes (signatures, handwriting). This legislative expansion provides clear legal sanction for investigative authorities to collect data that can be critical in solving modern, complex, and heinous crimes, directly strengthening the admissibility of scientific evidence in court.

The Supreme Court, even under the old regime, had recognized that certain involuntary physical evidence did not violate the right against self-incrimination (Article 20(3)). The Act formalizes

this position by making the collection of measurements compulsory and providing for legal action against resistance (Section 6). The implementation of the science and technology during the detection and investigation of the and administration of just oldest thing to the India[5]. Now the remodel technologies in the criminal profiling changes very fast by the new technologies and methods like DNA test, high performance liquid Chromatography, mass spectrometry, 3D computer[6] imaging and other sophisticated technologies are used by the Technologist and a scientist to reconstruct the offence and the crime area

Narco- Analysis Test

Narco analysis test is a state of Stupor induced by the drugs. The use of narcotics as a therapeutic aid in psychiatric is believed from the history of yearly Egyptians some of the medical doctors started to use scopolamine together with morphine and chloroform to provoke a state is called 'twilight sleep' in this limelight the test exposed in the Criminal Investigation.[7] Sekharan Vs State of Kerala[8] The high court of Kerala different approach towards the process and declaring unequally that is against the fundamental rights of the constitution and the right of the accused. The aspects of narco analysis permissible practise but it should not violate the self-incrimination was ensured in the Part III of the constitution.[9]

VI. CREATION OF CENTRALISED AND LONG TERM DATA BASE

The Act designates the National Crime Records Bureau (NCRB) as the central agency to collect, store, preserve, share, and disseminate the records of measurements. This centralization ensures

Inter-State Crime Detection: Facilitates the cross-verification of data across all states and Union Territories, which is vital for identifying suspects who operate across jurisdictions.

Long-Term Utility: Records can be stored for 75 years, enabling cold case investigations and the identification of repeat offenders over extended periods.

Judicial Oversight in Data Retention: While records are mandated to be destroyed upon acquittal or discharge, Section 4 allows a Magistrate or court to direct the retention of these records for recorded reasons. This judicial check prevents the premature destruction of potentially crucial data in cases of complex or ongoing investigations, maintaining the integrity of the database while retaining judicial oversight.

[5] B.B Nanda and R.K Tiwari, Forensic Science in India. A vision for the 21st Century 28
[6] "Innovative techniques of forensic science visited 23.11.2025"
[7] P. Ramanatha Aiyer's law lexicon 3121, Edition 2005
[8] 1980CRILJ31
[9] Chandan Panalal Jaiswal vs State of Gujarat 2004

 [ISSN 2581-5369]

VII. ENHANCEMENT OF INVESTIGATION AND CONVICTION RATES

A core stated objective of the Act is the direct improvement of the criminal justice system's output: crime detection and conviction. Broader Ambit of Persons (Section 3): The power to collect measurements is expanded to all convicts, arrested persons (for any offense), and even persons required to give security for good behaviour. This wider net ensures that identification data is systematically collected at the first point of contact with the law, creating a comprehensive database that significantly aids in linking suspects to past crimes when they re-offend.

Magisterial Power to Aid Investigation (Section 5): The Act empowers a Magistrate to direct any person to give measurements to aid an investigation or proceeding. This provision is vital for obtaining samples from witnesses or others who might be crucial for the case but are not accused, ensuring that no potential source of evidence is overlooked due to lack of specific legal mandate.

Increased Investigative Speed: The shift to centralized, digitized data processing facilitates faster matching of samples found at crime scenes, significantly expediting the identification process and the subsequent investigation. This is expected to directly contribute to the stated governmental goal of increasing the national conviction rate. The major emerging technologies include biometrics, facial recognition, DNA profiling, digital surveillance, AI-based criminal identification, and predictive policing mechanisms such as movement or intent detection.

1. Biometrics

Biometrics refers to the scientific method of identifying individuals using unique biological features such as fingerprints, iris patterns, voiceprints, and palm prints. These characteristics are stable, difficult to duplicate, and highly reliable[10]

National Automated Fingerprint Identification System (NAFIS): Integrates all states' fingerprint databases and enables nationwide search and matching.

Aadhaar-linked identification systems: Although Aadhaar is not used for criminal investigations directly, police agencies often rely on biometric verification for locating missing persons, unidentified bodies, and tracking habitual offenders.

Border management: Biometric gates and smart identity verification under the Immigration, Visa and Foreigners Registration & Tracking (IVFRT) system.

[10] A Comments on Selvi Vs State of Karnataka - 2010

 [ISSN 2581-5369]

2. Facial Recognition Technology (FRT)

Facial Recognition uses algorithms to compare a person's face with images stored in a database to confirm identity or detect suspects.

National Automated Facial Recognition System (NAFRS): Modern pan-India system under development to link CCTV feeds, police databases, and crime records.

State-specific systems: Telangana's TSCOP app, Delhi Police's FRS, and UP's Trinetra.

Public surveillance: Airports, metro stations, and high-security zones use FRT for real-time monitoring and threat detection.

3. DNA Profiling[11]

DNA profiling is a scientific process of identifying individuals using their genetic material. It is one of the most accurate tools for solving crimes, especially sexual offences, homicide, and disaster victim identification.

DNA labs: Expansion of DNA laboratories under the Ministry of Home Affairs and the Nirbhaya Fund.

DNA Regulation Bill (proposed): Aims to create a legal framework for DNA databanks.

Use in criminal trials: DNA evidence is increasingly accepted in courts for establishing guilt or innocence.

In the famous case of Gautam Kundu Vs West Bengal[12] the supreme court has laid down the certain guidelines regarding the DNA test and their admissibility in the Parentage case.

1. The courts in India cannot order blood test as a matter of course.
2. There must be a strong prima facie in this case in which the husband or any person must have established non access in order to dispel the presumption arise in under the section 112 Indian Evidence Act 1872.
3. Whenever the applications made for such prayer in order to having roving enquiry the prayer of blood test cannot be entertained in the court.
4. No one can be compelled to give blood samples for analysis in the criminal investigation.

[11] Yawer Qazalbash, law of lie Detectors – Universal Law Publishing Co., New Delhi, 2011
[12] (1993) 3 SCC 418

 [ISSN 2581-5369]

5. The court should carefully examine as to what would be the consequence of ordering the blood test during the investigation

In the case of Kanti Devi Vs Poshi Ram[13] The Honourable Supreme Court held that even DNA test the indicator the person is not a father of the child or the accused person is not involved in the crime. It would not be enough to rebut the conclusiveness of marriage as proof of legitimacy of child or the guilty person in the crime. The similar matter in the case of Rajiv Gandhi Murder Case[14] the DNA samples of allegedly assassin Dhanu were compared with her relatives, which gave conclusive proof about her being involved in the attack. Similarly in the famous Tandoor murder case[15] the DNA samples of victim Naina Sahni were compared with that of her parents to establish her identity.

4. Digital Surveillance[16]

Digital surveillance involves using CCTV cameras, drones, body-worn cameras, GPS trackers, mobile location data, and cyber-monitoring tools to observe and record activities for law enforcement.

5. AI-based Criminal Identification

Artificial Intelligence (AI) enhances the ability of law enforcement agencies to detect patterns, analyse large datasets, and identify suspects more efficiently.

Crime and Criminal Tracking Network & Systems (CCTNS): AI-enabled data analytics for faster detection of inter-state and repeat offenders.

6. Movement & Intent Scanning (Predictive Behaviour Analysis)

These technologies use video analytics, sensors, and AI to detect suspicious movement, behaviour, or potential threats before a crime occurs.

Smart CCTV analytics: Airports, metro stations, and railway stations use AI to detect abandoned objects, unusual crowd movement, and aggressive behaviour.

Integrated Command and Control Centres (ICCC): Part of the Smart Cities Mission, allowing real-time monitoring of citywide activities and rapid police response.

Proactive policing tools: Some state police are testing algorithms that predict potential offenders or crime zones.

[13] AIR 2001 SC 2026
[14] AIR 1993 SC
[15] 2007CRILJ4008, 2007 CRI. L. J. 4008, 2006 (12) SCC 421, (2007) 1 JCC 765 (DEL)
[16] Dr. B.R Sharma, Forensic Science in Criminal Investigation and Trial 4

 [ISSN 2581-5369]

Brain Mapping or P300 Test:

The brain mapping is the technique is also called as the 'brainwave finger printing'. It is the methodology to interviewed and interrogated to find out the whether the he is concealing an important information or not. The sum of the sensors is attached to the head and the person is made to sit in front of the computer monitor and we will identify it whether the person has to be guilty or not.

Finger Prints:

All human beings are born with a characteristics set of ridges on the fingertips. The ridges include rich in sweat pores, form a pattern that remains fixed for life. Even if the skin is removed the same pattern will be the great evidence when the skin regenerates. Some of the typical patterns found in fingerprints are arches, loops and whorls.[17]

VIII. A HUMAN-RIGHTS-ALIGNED EVALUATION OF THE CRIMINAL PROCEDURE (IDENTIFICATION) ACT, 2022

The Criminal Procedure (Identification) Act, 2022 represents a modern, human-rights compatible legal framework that enhances India's criminal justice system. When read with its Rules, the Act conforms to global human-rights norms such as the UN Principles on Data Protection, and the UN Guidelines on Crime Prevention.

1. Alignment with the UN Principles on Data Protection and Privacy (1990)

The UNDP Principles emphasise legitimacy, necessity, proportionality, accuracy, retention limits, and accountability.

The CPIA 2022 aligns with these principles in the following ways:

a) Lawful and Legitimate Purpose: The Act authorises data collection only for criminal identification, fulfilling the UN requirement that data must have a legitimate state purpose.

b) Proportional Use of Technology: Only persons involved in criminal justice proceedings are subjected to measurements. The Act uses biometric and behavioural data only to establish identity, not for mass surveillance.

c) Limited Retention Period (75 years): Though long, it ensures intergenerational crime tracking, essential for habitual offenders, sexual offenders, and absconders UN principles permit longer retention if justified for public security and crime prevention, which is fully satisfied here.

[17] "Fingerprint utility in forensic science" – Visited at 24.11.2025

 [ISSN 2581-5369]

d) Accountability through National Crime Records Bureau (NCRB): NCRB's centralised monitoring reflects UN-recommended independent oversight and secure digital storage mechanisms.

2. Consistency with the International Covenant on Civil and Political Rights (ICCPR, 1966)

ICCPR protects rights to privacy, dignity, fair trial, equality before law, and non-arbitrariness. The CPIA structurally respects these rights:

a) Article 17 – Right to Privacy: The Act mandates scientific and non-invasive procedures such as iris, fingerprint, or biological samples were authorised by law. Interference is lawful, necessary, and proportionate—the three-part ICCPR test.

b) Article 14 – Fair Trial and Due Process: Identification ensures accuracy of evidence, reducing reliance on coerced confessions and eliminating wrongful convictions. This advances the ICCPR obligation of fair and efficient prosecution.

c) Article 9 – Protection Against Arbitrary Arrest: By scientifically establishing identity, the Act prevents: mistaken arrests, misidentification, malicious prosecution. Thus it ensures precision in criminal procedure.

d) Article 2 – Equality and Non-Discrimination: Uniform standards for data collection mean: no profiling, no discrimination, equal treatment for all persons under criminal process.

3. Alignment with UN Guidelines for Crime Prevention (1995)

UN guidelines require states to adopt evidence-driven, scientific, and proactive crime-prevention strategies. The CPIA 2022 implements exactly that by: Replacing outdated 1920 Identification Act, Enabling DNA, fingerprints, iris, and behavioural profiling, Integrating AI-supported identification tools lawfully, supporting victim-centred justice by increasing crime detection rates, preventing repeat offenders from escaping identification. The Act therefore modernises India's crime-prevention system in line with global norms.

WHY THE ACT IS IMPORTANT FOR CRIME PREVENTION

a) Enhances accuracy in investigations

b) Prevents wrongful arrests and wrongful convictions

c) Increases conviction rates in serious crimes

d) Supports speedy justice

e) Protects vulnerable groups

 [ISSN 2581-5369]

IX. A POSITIVE REFORM AGENDA FOR THE CRIMINAL PROCEDURE (IDENTIFICATION) ACT 2022

1. Establish an Independent "Biometric Data Oversight Authority"[18]

To increase transparency, public confidence, and rights protection. Create a statutory oversight body (similar to UK Biometrics Commissioner). The authority will audit NCRB databases, verify lawful access, check deletion requests, and ensure compliance with proportionality requirements. Positive framing: "This will strengthen citizens' trust and enhance the credibility of the Act."

2. Introduce Periodic Review of Retention Period (75 years)

Conduct a review every 10 years to assess whether retention duration remains justified. Enable early deletion for persons acquitted or discharged unless required for national security. Positive framing: "This ensures the Act evolves with technological advancements while maintaining strong protections."

3. Mandatory Annual Transparency Reports by NCRB

NCRB must publish statistics on number of measurements collected, how many were used for crime detection, deletion requests and approvals, technological improvements. Positive framing: "This increases public awareness and demonstrates the Act's effectiveness in preventing crime."

4. Strengthen Data Security Protocols and Encryption Standards

Introduce mandatory end-to-end encryption, intrusion-detection systems, and annual cybersecurity audits. Mandate compliance with international gold standards (ISO/IEC 27001). Positive framing: "This ensures the Act remains technologically robust and aligns with global best practices."

5. Develop a Citizen-Friendly Redressal Mechanism

Allow individuals to request correction, deletion, or review of their biometric record through an online portal. Create a 30-day time limit for grievance resolution. Positive framing: "This promotes transparency and reassures citizens that their rights are fully respected."

[18] "DNA Test and its relevance in forensic science"

 [ISSN 2581-5369]

X. Digital security and data immutability via trust technologies

Block chain/Distributed Ledger Technology (DLT): While not explicitly mentioned, the implementation of a DLT layer on the NCRB database could provide data immutability. Every record entry, modification, or sharing action could be cryptographically recorded on a private DLT, ensuring an auditable and unalterable chain of custody. This robust mechanism directly addresses potential challenges related to data tampering and security, fortifying the evidence against judicial scrutiny.

Quantum Resistance Encryption

Given the 75-year retention period, the Act's implementation necessitates investment in Quantum-Resistant Cryptography standards to future-proof the database against decryption risks posed by quantum computing advancements, securing India's forensic assets for generations.

XI. Doctrinal foundation of technology – driven identification in india's criminal justice system

1. Doctrine of Proportionality (4-Pronged Test)

The proportionality test is the strongest doctrinal tool to justify technological expansion in criminal law.

a) **Legitimate Aim:** The State aims to prevent crime, strengthen identification procedures, and enhance national security.

b) **Rational Connection:** Digital biometrics, DNA profiling, and scientific measurements are rationally connected to efficient policing and accurate offender identification.

c) Necessity: Modern crimes (cybercrime, organised crime, transnational crimes) require advanced tools that older laws (1920 Act) could not support.

d) Balancing (Least Restrictive Means): Although the Act expands data collection, it does so to promote public safety and crime control—benefits outweigh minimal intrusion when safeguards exist.

The Act largely satisfies the proportionality test because scientific identification is a less intrusive alternative to arbitrary policing.

2. Doctrine of State's Positive Obligations (Article 21)

The right to life includes the right to protection from crime. The State has a positive duty to use effective tools to safeguard citizens. Using advanced technologies like biometrics, DNA, and

 [ISSN 2581-5369]

iris scans strengthens the State's obligation to ensure public safety. The CP(I) Act enables faster identification of offenders, preventing repeat offences and improving conviction accuracy.

3. **Doctrine of "Procedural Due Process"**

This helps you justify that the Act provides a structured, rule-based framework—better than the vague colonial 1920 Act. The Act lays down who can collect data, how it can be collected, and which authority stores it (NCRB).Scientific identification avoids arbitrary or subjective identification by police. Digital records bring transparency and standardisation in criminal investigation. Thus, the Act strengthens due process by reducing human error and eliminating outdated manual practices.

4. **Doctrine of "Compelling State Interest"**

Used in constitutional review to justify restrictions on individual rights if the State goal is extremely important. Preventing crime, combating terrorism, tracking habitual offenders, and improving public safety are compelling State interests. Emerging technologies significantly enhance identification accuracy and reduce wrongful arrests. The Act helps fight modern crime patterns which cannot be addressed through the 1920 framework. Thus, the Act survives constitutional scrutiny because it serves a critical public interest.

5. **Doctrine of "Reasonable Classification" (Article 14)**

To defend the expanded scope of data collection. The Act creates a reasonable classification between individuals involved in criminal processes and ordinary law-abiding citizens. Such classification is based on intelligible differentia (persons involved in crime) and has a rational nexus with the objective of crime prevention. This doctrinal tool helps show that the Act is not arbitrary.

6. **Doctrine of "Public Trust"**

This doctrine says the government must act for the welfare and protection of the public. By enabling scientific identification, the Act improves investigation quality and strengthens public confidence in the justice system. Misidentification and wrongful arrests reduce, enhancing trust in policing.

By applying doctrinal tools such as proportionality, compelling state interest, and scientific reliability, the Criminal Procedure (Identification) Act, 2022 can be seen as a progressive step that strengthens crime prevention through modern technology while maintaining constitutional safeguards.

 [ISSN 2581-5369]

XII. CONCLUSION

The Criminal Procedure (Identification) Act of 2022 marks an important transition from the colonial-era 1920 Act to a modern, scientifically sound justice system. By integrating modern biometrics and providing the NCRB with unified data management, the Act addresses the fundamental "evidence deficit" that has long hindered conviction rates. This research validates the Act's constitutional validity. The State's compelling interest in public safety and accurate crime detection overcomes the modest privacy invasions, effectively meeting the Proportionality doctrine. The change from relying on faulty eyewitness testimony to immutable scientific evidence boosts prosecutions while simultaneously protecting civil liberties by reducing unjust arrests. However, in order to maintain public trust, any technological advancement must be supported by significant safeguards such as independent oversight and strict confidentiality of information. Ultimately, the Act is an essential evolution for ensuring a precise, efficient, and truth-oriented criminal justice ecosystem. The emerging technologies in criminal profiling in the criminal justice system with the help of DNA profiling, polygraphy and taking measurements of the accused person under the Criminal Procedure Identification Act 2022 involve reducing the number of crimes in the contemporary era, like murder, rape, robbery, dacoity, etc. Criminal profiling solved the unsolved crime. However, our legal system was framed at a time when such modern scientific techniques had neither developed nor been foresighted. But now the modern digital world and artificial intelligence have been involved in the criminal profiling, and there has been more accuracy and precision in the actual fact and circumstances while conducting the investigation and examination of a person. The Criminal Procedure Identification Act 2022 the criticism put forward by the legal expert on the ground did violate the fundamental rights of a person under the article 20(3) and 21 does not seem justified thus, one should not only be concerned with the protection of fundamental rights and integrity in the criminal investigation but also should see the rights of the person violated in order for the measurements taken by the Criminal Procedure Identification Act to be subordinate to fair and speedy justice.

The Criminal Procedure (Identification) Act, 2022, represents a paradigm shift from outdated anthropometric approaches to cutting-edge biometric and artificially intelligent identification, bring India's criminal justice system in line with worldwide technological standards. While the Act improves investigation speed and conviction rates, its broad reach and potential for mass surveillance raise valid concerns about privacy, data security, and prejudice. The ultimate success of this legislation will be determined not by its technological ambition, but by strong safeguards, transparent execution, and continuous judicial scrutiny. India can set a worldwide

 [ISSN 2581-5369]

standard for balancing public safety and individual liberty in the digital era by implementing a rights-centric approach that includes time-bound data retention, independent audits, and consistency with the expanding data protection regime.

1. Time-bound Retention Policy with Judicial Oversight and Introduce a statutory mandate that biological samples and measurement data of acquitted persons or those not charged must be destroyed within 90 days, with mandatory certification by a Judicial Magistrate to prevent misuse and ensure compliance with Article 21.
2. Mandatory Data Protection Impact Assessment (DPIA) and make it compulsory for NCRB and state forensic agencies to conduct and publish annual DPIA before expanding the scope of technologies like facial recognition, iris scans, gait analysis, etc. under the Act, in line with the Digital Personal Data Protection Act, 2023.
3. Establish an Independent Forensic & Biometric Oversight Board and Constitute a multi-disciplinary Board like comprising judges, technologists, civil society, forensic experts to periodically audit the accuracy, bias, and proportionality of AI-based identification systems deployed under the 2022 Act.
4. Narrow the Definition of "Measurement" through Rules and the Central Government must notify strict Rules within six months defining "behavioural attributes" and explicitly excluding controversial technologies e.g., narco-analysis, brain mapping) and limiting facial recognition only to high-quality CCTV footage to avoid overreach.
5. Mandatory Training and Certification of Police Personnel. No police officer below the rank of Sub-Inspector should be authorised to collect measurements unless certified through a standardised NCRB training module on privacy, consent, and scientific limitations of biometric technologies.
6. Special Safeguards for Vulnerable Groups like Children, women, transgender persons, and tribal communities must be given additional protections, measurements only in the presence of a parent/legal guardian or social worker, and explicit prohibition on retaining data beyond case disposal.
7. Integration with Criminal Justice CrPC & BNSS Reforms and Harmonise the 2022 Act with the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) by mandating that refusal to give measurements can only be treated as circumstantial evidence (not presumptive guilt) and cannot be the sole basis for prolonged detention.

 [ISSN 2581-5369]

8. Public-Private Partnership Transparency Framework. Any use of private-sector AI/biometric solutions (e.g., by companies providing facial recognition) must be governed by a transparent tender process and annual third-party security audits, with results placed before Parliament.

*****

 [ISSN 2581-5369]

XIII. REFERENCE:

BOOKS:

1. P.K. Majumdar, Law of Bails, Bonds and Arrest 2012 (Orient Publication)
2. P.V. Ramakrishna, Law of Bail, Bonds, Arrest and Custody 2008 (LexisNexis)
3. Ratanlal & Dhirajlal, Criminal Procedure,2012 (Lexis Nexis Butterworths Wadhwa, Nagpur
4. K. I. Vibhute, Criminal Justice A Human Rights Perspective of the Criminal Justice
5. Doald R. Taft and Ralf W. England, Criminology, 1964

ARTICLES:

1. Prof.Dr Priya Sepaha, Criminal profiling of pshycopaths, 3,2022
2. Kaustubh Phalke, Criminal profiling and how it is used, blog.ipleader , (24.11.2025, https://blog.ipleaders.in/all-about-criminal-profiling
3. Adya aditi Samal, minds in the Shadow – forensic profiling , 36, 2021
4. From crime scene to Conviction- Criminal profiling in india, Jyothi Judiciary, (24.11.2025).

CASE LAWS:

1. Prakash Singh v. Union of India (2006) 8 SCC 1 242
2. Prison Statistics India Report 2015, National Crime Records Bureau.
3. Rama Murthy v. Karnataka, AIR 1997 SC 1739 253
4. State of Maharashtra v Prabhakar Pandurang Sangzgiri and another AIR1966SC424
5. Francis Coralie Mullin v The Administrator, Union territory of Delhi and Others AIR 1981SC746
6. State of Maharashtra and others v Asha Arun Gawali and another AIR 2004SC2223
7. State of Gujarat and another v Hon'ble High Court of Gujarat AIR1998SC3164
8. R.D Upadhyay v State of Andhra Pradesh AIR2006SC1946

*****

 [ISSN 2581-5369]