THE CRIMINAL PROCEDURE (IDENTIFICATION) ACT, 2022: A CRITICAL ANALYSIS OF ITS LEGAL, CONSTITUTIONAL, AND SOCIETAL IMPLICATIONS

N R Divyashree, Assistant Professor of Law, MKPM RV Institute of Legal Studies, Bangalore

ABSTRACT

The Criminal Procedure (Identification) Act, 2022 marks a significant overhaul of India's legal framework concerning the identification of individuals involved in criminal proceedings. Replacing the Identification of Prisoners Act, 1920, the new legislation substantially broadens the scope of data collected from individuals, including convicts, detainees, and even certain arrested persons. This paper critically analyzes the legal framework of the Act, explores its constitutional validity in light of privacy and human rights concerns, examines the potential for misuse, and considers its implications in the context of modern criminal justice systems. It also offers recommendations for balancing state interests with individual liberties.

Keywords: Criminal Procedure (Identification) Act, 2022, Fundamental Rights, Legal Implications

1. Introduction

The Criminal Procedure (Identification) Act, 2022 was enacted by the Indian Parliament to authorize the collection of certain identifying information from persons involved in criminal matters. This Act replaces the colonial-era Identification of Prisoners Act, 1920, which was considered outdated in the context of modern policing, forensic sciences, and technological developments. The new law allows for the collection of biometric data such as finger impressions, palm prints, foot prints, iris and retina scans, physical and biological samples, and behavioral attributes including signature and handwriting.

2. Key Features of the Act

The Act defines "measurements" broadly to include finger impressions, palm-print impressions, foot-print impressions, photographs, iris and retina scans, physical and biological samples, and their analysis, as well as behavioral attributes like signature and handwriting. Its scope applies not only to individuals convicted of any offense, but also to those ordered to give security for good behavior or maintenance of peace, and even to individuals arrested for crimes, particularly offenses against women or children or those punishable with imprisonment exceeding seven years.

The National Crime Records Bureau (NCRB) has been given the responsibility of collecting, storing, and preserving the data, and can share such records with law enforcement agencies as necessary. The records are to be stored in a centralized system, enabling efficient cross-referencing, monitoring, and data analysis. This integration is intended to strengthen law enforcement’s ability to link suspects to multiple cases and use biometric identification to track criminal movements across regions.

A critical point of contention is the provision for data retention, which permits storage for up to 75 years. The Act is silent on deletion protocols, even in cases of acquittal or discharge, raising significant concerns over data misuse and privacy violations. Moreover, refusal to provide such data is treated as an offense under Section 186 of the Indian Penal Code. This criminalizes non-compliance even when the subject may have legitimate grounds for resistance.

3. Legal and Constitutional Concerns

The right to privacy, established as a fundamental right under Article 21 by the Supreme Court in *Justice K.S. Puttaswamy v. Union of India* (2017), is potentially undermined by the sweeping powers granted under the Act. The absence of clear limits on data types, collection purposes, and access controls creates a fertile ground for overreach. The collection of data from individuals who are not yet convicted fails the tests of necessity and proportionality, which are central to privacy jurisprudence.

Article 20(3) of the Constitution provides protection against self-incrimination. Traditionally, this protection does not extend to physical evidence, but the inclusion of behavioral attributes such as handwriting and voice samples may raise complex legal questions. These samples can be argued to be testimonial in nature, thereby attracting constitutional protection. The lack of clear judicial interpretation on this matter adds to the ambiguity. If handwriting analysis can imply mental intent or link to a confession, it could be said to cross into testimonial evidence.

Furthermore, the Act lacks procedural safeguards. It authorizes police and prison officers to collect data without requiring prior judicial approval, unlike other criminal procedures such as searches or interrogations. This creates a scenario where individuals could be subjected to invasive procedures based solely on police discretion. Additionally, the Act fails to establish an independent authority for grievance redressal or procedural checks, thereby weakening accountability. There is a growing demand for oversight bodies that can review and audit the procedures followed during data collection.

The use of vague terminology, particularly the undefined scope of "biological samples," compounds the issue. Such terminology could be interpreted to include highly intrusive methods such as blood tests or DNA profiling, with no accompanying safeguards. This undermines bodily autonomy and the principle of least intrusive intervention. Without legislative precision, these terms may be interpreted expansively, leading to abuse under the guise of legality.

4. Comparative Legal Perspectives

A comparative examination reveals how other democracies manage similar legislative frameworks. In the United Kingdom, the Protection of Freedoms Act, 2012 mandates the deletion of biometric data for individuals not convicted of crimes. This reflects a rights-based approach where data collection is accompanied by procedural safeguards and limited retention

periods. The UK's legislative architecture underscores the importance of proportionality and individual rights.

In the United States, the Fourth Amendment protects against unreasonable searches and seizures. While biometric data can be collected, it is usually subject to warrants or judicial scrutiny. The judiciary serves as a gatekeeper, ensuring that fundamental rights are not overridden by executive expediency. The practice of requiring judicial authorization introduces a level of procedural fairness that India's current framework lacks.

The European Union's General Data Protection Regulation (GDPR) represents the gold standard in data privacy. Biometric data is classified as sensitive personal information and can only be processed with stringent safeguards, including the individual's right to access, correct, and delete their data. States must demonstrate that such processing is necessary and proportionate to the purpose. GDPR also enshrines the principle of data minimization and storage limitation, mandating that data should not be retained longer than necessary.

By contrast, the Criminal Procedure (Identification) Act, 2022 lacks any of these detailed protections, making it more susceptible to abuse and less protective of individual freedoms. India's approach, as it stands, is enforcement-heavy with insufficient emphasis on constitutional balance and privacy ethics.

5. Implications for Law Enforcement and Society

From a law enforcement perspective, the Act provides a more sophisticated framework for identifying and tracking individuals involved in criminal activities. Centralized data storage and advanced analytics could enhance crime detection and reduce recidivism through better profiling. It also allows better interstate coordination of criminal investigations and builds a repository of forensic intelligence. Such tools can be extremely valuable in combating organized crime and terrorism.

However, the risks are equally significant. The expanded powers could lead to disproportionate targeting of marginalized communities, reinforcing existing systemic biases. The specter of mass surveillance looms large, especially in the absence of oversight mechanisms. Public trust in law enforcement may erode if individuals feel their data is being collected indiscriminately or misused. Furthermore, the lack of robust cybersecurity frameworks heightens the risk of

data breaches, with potentially grave consequences for individuals whose sensitive information is compromised.

The inclusion of undertrials and individuals merely arrested but not convicted is particularly problematic. In the Indian context, where pre-trial detention can be prolonged and acquittal rates are high, the stigmatization caused by retaining such data can result in social and economic exclusion. Without automatic deletion or sealing mechanisms post-acquittal, these individuals face continued harm despite judicial exoneration. This challenges the principle of presumption of innocence and has broader implications for rehabilitation and reintegration into society.

6. Recommendations

To reconcile the objectives of effective law enforcement with the imperatives of civil liberty, the Act must be supplemented by robust legal and institutional safeguards. A comprehensive data protection law should be enacted that governs the collection, storage, and use of biometric data. This would provide a legal framework for privacy protection and empower citizens with rights such as access and correction. The inclusion of these elements is not merely procedural but essential to democratic governance.

Judicial oversight should be introduced, particularly for the collection of invasive biological samples. Magistrate approval should be made mandatory in such cases to ensure accountability and prevent arbitrary action. Additionally, the Act should prescribe clear timelines and procedures for the deletion of data for those not convicted, thereby preventing the long-term stigmatization of innocent individuals. These reforms would bring Indian law in alignment with international human rights standards.

An independent oversight authority must be established to regulate the functioning of the Act. This body should be empowered to audit data usage, investigate complaints, and ensure compliance with due process. Law enforcement personnel should also be sensitized through training programs to uphold ethical standards and human rights while implementing the Act. Public awareness campaigns can further ensure transparency and build trust among citizens.

7. Conclusion

The Criminal Procedure (Identification) Act, 2022 is a landmark legislation with the potential

to transform the investigative landscape in India. While it promises enhanced efficiency in crime detection, it simultaneously presents profound challenges to constitutional freedoms. The key lies in implementing the Act with a clear commitment to human dignity, privacy, and justice. Through the introduction of safeguards, judicial oversight, and a culture of accountability, the Act can be aligned with the broader goals of a democratic and rights-respecting society. Future amendments must be guided by dialogue with legal experts, civil society organizations, and data protection authorities to ensure the law evolves to meet both enforcement goals and human rights standards.

References:

- The Criminal Procedure (Identification) Act, 2022
- The Constitution of India
- Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1
- Protection of Freedoms Act, 2012 (UK)
- General Data Protection Regulation (EU)
- Project 39A Research Briefs
- International Journal of Current Science, IJCSP24B1035
- Indian Journal of Integrated Research in Law, 2023