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

VOLUME 6 AND ISSUE 3 OF 2026

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

Published by

Institute of Legal Education

https://iledu.in

ANALYSIS OF FORENSIC FINGERPRINTING IN CRIMINAL INVESTIGATION: PRIVACY CONCERNS AND LEGAL SAFEGUARDS IN INDIA

AUTHOR – BHUVANESH M* & SUGITH KUMAR RG**

* STUDENT AT SCHOOL OF EXCELLENCE IN LAW, TNDALU

** PROFESSOR AT SCHOOL OF EXCELLENCE IN LAW, TNDALU

BEST CITATION – BHUVANESH M & SUGITH KUMAR RG, ANALYSIS OF FORENSIC FINGERPRINTING IN CRIMINAL INVESTIGATION: PRIVACY CONCERNS AND LEGAL SAFEGUARDS IN INDIA, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (3) OF 2026, PG. 3110-322, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT:

The forensic fingerprint has for long been considered as one of the most reliable scientific methods of personal identification in criminal investigations. Fingerprint evidence in India has been used extensively for identifying and connecting the suspects to the crime scenes, and record keeping of a criminal. But the digitisation of forensic systems and creation of biometric databases has widened the scope of digitisation and storage of fingerprints by Law Enforcement Agencies. While these developments are aimed at simplifying investigations, they are not devoid of constitutional challenges in the areas of privacy, personal liberty and protection of biometric data. With the Indian Supreme Court recognising the right to privacy as a fundamental right in Justice K. S. Puttaswamy (Retd.) v. Union of India, the issue of biometric data collection and storage warrants a closer legal attention.

The current research paper focuses on the doctrinal analysis over the existent legal framework on forensic fingerprinting of the Indian subject. The research paper has considered the main provisions of Criminal Procedure (Identification) Act, 2022 and the related constitutional jurisprudence, which has been taken into account by the courts. The study reveals that forensic fingerprint is a scientific procedure that has evolved over time and has become an instrument of criminal investigation. The existing legal framework particularly in the context of biometric data and this paper finds that there is no comprehensive safeguard over the biometric data in terms of data retention, oversight and proportionality. The study suggests that a rights-based regulatory framework over biometric data must be elaborated, which ensures the balance between criminal investigation, personal liberty, dignity and privacy.

Keywords: Forensic fingerprinting, Personal Liberty and Dignity- Constitutional Safeguards- Biometric Evidence Regulation- Privacy Jurisprudence in India- Law Enforcement Surveillance

INTRODUCTION:

The administration of criminal justice in any constitutional democracy is contingent upon the ability of the State to correctly identify individuals as well as to protect fundamental rights. Of various scientific techniques of personal identification, forensic fingerprinting is one of the longest surviving and most accepted tools of criminal investigations. In the context of uniqueness, permanence and individuality of fingerprint patterns, fingerprint evidence has traditionally been viewed as a reliable means of linking suspects to crime scenes, verifying identities and maintaining criminal records. In India, forensic fingerprinting has played a central role in investigative activities since the

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

VOLUME 6 AND ISSUE 3 OF 2026

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

Published by

Institute of Legal Education

https://iledu.in

colonial period and continues to be at the centre of contemporary policing and judicial processes.

In recent decades, the role of forensic fingerprinting underwent a radical change. What was once a case-specific forensic technique has been transformed into a digitised and centralised system of biometric identification, underpinned by automated databases and sophisticated technological infrastructure. Law enforcement agencies can now collect, store, analyse and retrieve fingerprint data at an unprecedented scale. While such developments have undoubtedly helped in expediting and improving the efficiency of criminal investigations, they have also expanded the scope of State surveillance and control over personal biological data[1].

Fingerprint data are a type of biometric information that is uniquely and unalterablely connected to the human body and a person's identity. Therefore, the protection of biometric identifiers is of utmost importance since they cannot be changed or substituted, as is the case with conventional personal data, if compromised. The retention of biometric data, especially the fingerprints of unconvicted persons, with no discernible limit or purpose, is in direct conflict with the fundamental principles of criminal jurisprudence, including presumption of innocence and due process of law. In the absence of explicit statutory rules regarding consent, retention, access and destruction of biometric data, forensic fingerprinting can easily move from legitimate investigation to unconstitutional intrusion. The growing recognition of the right to privacy as a fundamental right under the Indian Constitution has also brought biometric practices by the State under scrutiny. Privacy, being an essential element of the right to personal liberty, informational self-determination and bodily integrity, limits the scope of State power. Any encroachment upon this fundamental right must be lawful, necessary and proportionate. But the legal framework for forensic fingerprinting in India is in its infancy and fragmented, and is largely evidence-oriented in nature, rather than rights-oriented. This gap between the technological capabilities and legal accountability creates a regulatory void that leaves individuals vulnerable to misuse of sensitive biometric data.

Against this background, it is not possible to consider forensic fingerprinting used in criminal investigations purely from scientific or evidentiary point of view. It is important also to consider it in its wider constitutional context of privacy, surveillance and State power versus individual freedom. The research objective is to critically analyse the use of forensic fingerprinting in India by assessing its implications on the privacy right and the adequacy of the existing legal safeguards vis-a-vis the constitutional jurisprudence on privacy. By using the comparative legal perspective, the study also aims to identify gaps in the legal and constitutional framework and to recommend a coherent approach that maintains a balance between the fundamental rights and effective law enforcement.

SCOPE OF THE STUDY:

The scope of the present study is broad and multidimensional by design in order to critically appraise the forensic fingerprinting in the context of criminal investigations in the Indian legal system, and at the same time, respond to the growing concerns about individual privacy and data protection. The present study positions forensic fingerprinting as a highly venerable, widely used, and institutionalised biometric technique by law enforcement agencies in India.

This study focuses on fingerprint evidence as an investigative tool and as a form of personal biometric data to critically appraise how the role of technocratic certainty in criminal justice relates to constitutional values, especially those concerning the right to privacy, personal liberty, and human dignity. The present study analyses the legal basis of fingerprinting for collection, storage, analysis, and use in India. It also studies the statutory basis of law enforcement

agencies to collect fingerprints from the accused, convicts, and detainees, and, in few cases, from non-convicted persons. The study extends to a critical analysis of procedural safeguards in criminal law and how these are implemented. Through this, the present study critically evaluates whether the laws in force provide the right balance between effective criminal investigation and the individual's right to privacy.

A Critical Analysis of Constitutional Jurisprudence and Judicial Interpretation, Modern Law and Ethics. The study will critically examine the constitutional jurisprudence and judicial interpretation that has governed the legality of forensic fingerprinting in India. It will explore how courts have historically treated fingerprint evidence, its evidentiary value, and its admissibility in criminal trials. The scope will also extend to the evolving judicial understanding of privacy, particularly in the post-recognition era of privacy as a fundamental right, and how this evolution reshapes the legal and ethical legitimacy of compulsory fingerprinting.

By scrutinizing landmark judicial decisions, the study will evaluate if current forensic practices align with constitutional principles of proportionality, necessity, and procedural fairness. The research will also delve into the technological and administrative aspects of forensic fingerprinting, examining the collection, digitisation, classification, database integration, and long-term storage processes managed by forensic and policing authorities. This scope will address potential risks of misuse, unauthorised access, data breaches, function creep, and the absence of accountability mechanisms. The study will assess if India's forensic infrastructure has robust technical safeguards, oversight mechanisms, and data minimisation practices to prevent the exploitation of biometric data in the absence of a comprehensive personal data protection regime.

Finally, the study is also forward looking in nature in that it also extends to policy analysis and reform based discussion. It attempts to evaluate the adequacy of the existing legal safeguards and to make recommendations to enhance the privacy protections without adversely affecting the effectiveness of criminal investigations. This, therefore, expands the scope to include a review of the necessity for clearer statutory limits, an independent oversight body, norms for retention and deletion, informed consent standards where applicable, and judicial oversight of use of biometric data. In this expansive scope, the study intends to make a significant contribution to academic and legal reform discourses, and policy formulation in the area of forensic science, criminal justice, and constitutional rights in India.

REVIEW OF LITERATURE:

People have been debating how forensic identification - especially things like fingerprinting and other biometrics - fits with personal privacy for a long time. Lately, with police and governments relying more on these technologies, the conversation's only gotten louder. You've got scientists and legal thinkers both chiming in: some dig into how reliable fingerprint evidence is, others worry about what happens when authorities collect and keep huge databases of people's most personal information.

Way back in 1892, Francis Galton wrote Finger Prints[2], and that book pretty much set the rules for how we think about fingerprints — that they're unique, and that they last. Thanks to his work, police started using fingerprinting as a main tool for identifying suspects. Later, forensics experts like Henry C. Lee and R. E. Gaensslen kept building on that, diving into the science and tech behind fingerprint analysis. Their research makes it clear: fingerprinting really does help connect suspects to crimes.

But here's the thing. Legal scholars keep asking if all this biometric identification fits with constitutional rights. In India, the whole privacy debate took a big turn after the Supreme Court's Justice K. S. Puttaswamy (Retd.) v. Union

of India[3] decision. The Court said privacy is a fundamental right under Article 21. People like Gautam Bhatia, and the Srikrishna Committee on Data Protection, argue that if the government's going to collect sensitive stuff like biometrics, there have to be real safeguards.

Courts have also weighed in on whether the police can force you to give fingerprints. In State of Bombay v. Kathi Kalu Oghad[4], the Supreme Court said taking fingerprints isn't self-incrimination because it's physical evidence, not something you say. Still, plenty of scholars point out that gathering everyone's biometrics, and holding onto them, raises serious questions about privacy and freedom.

On top of that, academics have looked at the laws around fingerprint collection in India. The old Identification of Prisoners Act, 1920, let police take fingerprints and other measurements from certain suspects. Now, that's been replaced by the Criminal Procedure (Identification) Act, 2022, which gives the authorities much wider powers to collect biometrics. Critics aren't thrilled — they say the new law gives too much leeway to law enforcement, with not enough checks on how long they can keep your data, or who's watching over the whole process.

Looking beyond India, scholars like David Lyon have shown that while biometrics make it easier to identify people and improve security, these technologies can fuel surveillance if governments don't set clear limits. So, the big question keeps coming up in research and policy: how do we balance the real benefits of forensic fingerprinting with the need to protect privacy, dignity, and personal freedom?

HYPOTHESIS:

This paper hypothesises that although forensic fingerprinting is scientifically robust, it is being practised in a legal context that fails to give due consideration to the constitutional right to privacy. It hypothesises further that the failure to implement proportionate safeguards and adequate controls leads to an unwarranted violation of personal liberty.

RESEARCH METHODOLOGY:

This study explores the legal framework of forensic fingerprinting in criminal investigations in India through a doctrinal method of study. The enquiry is analytical and descriptive in nature and based on secondary sources such as constitutional provisions, statutes, case law, law commission reports, and other scholarship.

By critically examining legislation and case law this study explores the legal, admissibility and constitutional aspects of fingerprinting, especially as regards the right to privacy. Where relevant, comparative and international human rights materials are cited in order to evaluate the effectiveness of existing safeguards and to underpin reformative conclusions.

RESEARCH GAP:

Although a substantial body of literature exists on forensic science and biometric evidence, there is a notable lacuna in forensic science research in India on the intersection of forensic fingerprinting and newly emerging data protection jurisprudence. Most of the available literature focuses on a narrow set of issues on the evidentiary value of fingerprints or technical aspects of biometric classification, without addressing the broader constitutional and regulatory implications generated by biometric data collection, database retention, secondary use and governance in the post-privacy jurisprudence era.

It is particularly relevant for the contemporary state of Indian jurisprudence to ask how the Supreme Courts recognition of the right to privacy as a fundamental right in Puttaswamy v. Union of India has implications on the legal legitimacy of biometric practices such as mandatory fingerprinting in the absence of a comprehensive statutory data protection framework. And, in the absence of empirical and doctrinal research on how fingerprint databases are used beyond the immediate criminal investigation (e.g. data sharing with non- police agencies, retention post-acquittal, linkage with identity systems such as Aadhaar)

is it a case of function creep and disproportionate surveillance.

There is little legal scholarship on the procedural safeguards, oversight mechanisms and accountability mechanisms necessary to prevent fingerprinting from becoming a tool of unchecked state power. For example, little work has been done to explore procedural safeguards such as judicial authorisation thresholds, data minimisation norms, data retention and deletion policies, and remedies for misuse in the Indian context. Only a handful of studies have conducted comparative research with states that have comprehensive biometric data protection laws, such as the EU's GDPR framework, the UK's Biometrics Commissioner regime or the US's biometric privacy laws at the state level, and those that do are often not in depth.

The research gap is the lack of comprehensive, right-based legal scholarship on how forensic fingerprinting practices in India can be reconciled with privacy, data protection and constitutional rights, and what regulatory, institutional and procedural safeguards and, and accountability mechanisms need to be in place to achieve that balance.

RESEARCH PROBLEMS:

1. Whether the current legal framework for forensic fingerprinting in India provides sufficient and constitutionally sound safeguards to protect the fundamental right to privacy with regard to the collection, storage and use of biometric information.

2. Whether the discretionary powers of the law enforcement agencies in compulsory fingerprint collection lead to an excessive violation of the personal liberty, dignity and presumption of innocence, specifically of the undertrials and acquitted persons.

3. Determining whether a lack of clear statutory norms on data retention, deletion, purpose limitation and oversight would lead to misuse, function creep or long-term surveillance through fingerprint databases.

4. How adequate current judicial interpretations and procedural safeguards are for regulating forensic fingerprinting practices in the light of evolving privacy jurisprudence in India.

5. Whether India's forensic fingerprinting regime requires a special rights-based regulatory framework to ensure investigative efficiency while respecting constitutional and human rights obligations.

BACKGROUND OF FORENSIC FINGERPRINTING IN CRIMINAL JUSTICE:

One of the most significant milestones in the history of the use of science in the field of criminal justice is the use of forensic fingerprinting. The use of fingerprint identification is based on the principle that the pattern of ridges found on the fingers of every human being is unique to every individual. Furthermore, the pattern of ridges on the fingers of every person remains the same throughout their lifetime. This characteristic of fingerprints has made them one of the most powerful tools of identification for the purposes of associating an individual or persons with a particular object or crime.

EARLY ORIGINS OF FINGERPRINT IDENTIFICATION:

The use of fingerprints to identify individuals stretches back more than a thousand years before the emergence of modern forensic science. There is ample evidence that fingerprints were used in authentication by ancient societies. The ancient Babylonian people, around 2000 BCE, would press their fingerprints onto clay tablets in order to confirm the identity of parties in a commercial transaction and to authenticate agreements.

In China and early Japan, another ancient culture, fingerprints would occasionally be left on documents as a form of signature or to establish proof of identity. These early uses of fingerprints demonstrate that societies were aware, from at least 2000 BCE, that fingerprint patterns were unique. However, these early uses of fingerprints lacked a scientific basis or the classification of fingerprint patterns. In addition,

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 3 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

fingerprints were primarily used for administrative or commercial purposes and the fingerprints were not used for criminal identification. It was, however, not until the nineteenth century that investigators began to study fingerprints scientifically and to investigate the use of fingerprints in law enforcement.

RISE OF FINGERPRINT SCIENCE:

The scientific study of fingerprints began in nineteenth century with a number of researchers looking for reliable ways to identify persons. One of the most significant breakthroughs in the use of fingerprints occurred when the British administrator Sir William James Herschel[5] began conducting experiments on fingerprint identification while he was serving in India in the 1850s. In 1859, as the Chief Magistrate of the Hooghly district, Herschel realized that the contract makers needed to deposit either their hand prints or fingerprints on the documents. After a long period of experiments he hypothesized that the patterns of fingerprints are permanent over time and can be used to differentiate individuals.

Herschel's experiments proved two principles that are the basis of forensic fingerprinting: permanence and uniqueness of fingerprints. Although Herschel's experiments were initially aimed at preventing fraud in administrative processes rather than identifying a criminal, they provided the first empirical evidence for using fingerprints to identify individuals.

Further scientific development. The work of Henry Faulds. Scottish physician Henry Faulds published an article in 1880 proposing that fingerprints be used in identifying criminals and that fingerprints left behind at the scenes of a crime could be compared with the fingerprints of suspects. He suggested that fingerprints should be systematically classified and also engaged with scientists in regards to the use of this method in criminal investigations.

British scientist Francis Galton carried out extensive statistical studies of fingerprint patterns at around the same time. Galton's work helped scientificy validate fingerprint individuality and his classification of fingerprint patterns into three basic types (loops, whorls and arches) was incorporated in his influential publication Finger Prints (1892). This helped give fingerprint analysis a scientific basis and helped its use in the criminal justice system[6].

THE SHIFT FROM ANTHROPOMETRY TO FINGERPRINT IDENTIFICATION:

Before fingerprints, law enforcement used a process called anthropometry, which was pioneered by French criminologist Alphonse Bertillon. The system was a collection of measurements of parts of the human body, such as arm span, head length, ear size, etc. This system was used to identify repeat offenders. Anthropometry was an innovative process at the time, but it was not reliable.

There were cases where two people had similar measurements and also record keeping for the anthropometry measurements was difficult to maintain. Anthropometry was somewhat limiting and the need for a more reliable system was there. Fingerprints began to be used as the identification system because fingerprints are easier to keep and they are very unique to each person. The shift from anthropometry to fingerprints was a huge change in the ways in which forensics and crime scene investigations were conducted.

DEVELOPMENT OF THE MODERN FINGERPRINT CLASSIFICATION SYSTEM:

Sir Edward Henry made an important contribution to the application of fingerprint identification to the criminal justice system in the last part of the nineteenth century. While Inspector-General of Police in Bengal, Henry worked with the Indian police officers Qazi Azizul Haque and Hem Chandra Bose to develop a system of efficient classification and storage of fingerprint records.

They developed the Henry Classification System in 1896-97 which enabled fingerprint records to be stored and retrieved quickly. Mathematical

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 3 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

formula were developed to allow fingerprints to be classified according to pattern characteristics. Investigators were then able to search large databases of fingerprints. Henry's system provided a solution to the problem of dealing with large numbers of fingerprint records and thus marked the beginning of the modern fingerprint system of identifying criminals.

After a government committee recommended the use of fingerprints for identification, criminal identification by fingerprints was formally adopted by the British Indian administration in 1897. Fingerprinting supplanted anthropometric identification in India in 1900 and soon thereafter was implemented elsewhere in the world[7].

THE INSTITUTIONALIZATION OF FINGERPRINTING:

After India became a success story, fingerprint identification gained widespread international acceptance. Police organisations in Europe, North America and elsewhere began to set up fingerprint bureaus to hold criminal records. The first such bureau in the United Kingdom was created at Scotland Yard in 1901, signalling the institutionalization of fingerprint identification in modern policing.

Criminal courts throughout the twentieth century came to accept fingerprint evidence as a reliable form of forensic evidence and experts were routinely called to testify to the presence of suspects at crime scenes or to identity. Over time as forensic science developed, the fingerprint examiner became part of an integrated forensic investigative team, working closely with crime scene investigators, evidence collectors and laboratory scientists.

THE TECHNOLOGY OF FINGERPRINTING IN CRIMINAL INVESTIGATIONS:

The use of fingerprinting in criminal investigations has been further improved by technological advancement. Manual comparison of fingerprints was replaced by a computerized system which stored and performed analysis on millions of fingerprints. An Automated Fingerprint Identification System (AFIS) is now available to law enforcement agencies to compare fingerprints from crime scenes with national databases in seconds.

In India, the National Automated Fingerprint Identification System (NAFIS) was developed, which enhanced forensic identification. The National Crime Records Bureau manages the system, which allows law enforcement agencies to upload and search fingerprints throughout the country in real time. The database now includes more than 10 million criminal fingerprint records in 2024, speeding up the identification of suspects and unidentified persons[8].

FINGERPRINTS - PAST AND FUTURE:

The continuing importance of fingerprints in criminal investigations is, perhaps, an oxymoron. In a nice but a little outdated chapter of his book on fingerprint evidence, Kazar et al. (1977) concluded that "there is no doubt that fingerprint evidence is the most widely used forensic method of crime-scene investigation in the world, and this will continue to be true for the foreseeable future."

Since the time of Kazar et al., the forensic use of fingerprints has continued to receive wide adoptions while the use of DNA profiling continues to grow. There are always debates on personal privacy, data protection, data security and misuse of biometric and fingerprint data. This book addresses the current problems faced by forensic scientists in the age of DNA profiling. It also addresses the new challenges which forensic scientists face in maintaining the privacy of the biometric and fingerprint data. It addresses the new challenges which forensic scientists face in maintaining the privacy of the biometric and fingerprint data.

FINDINGS :

1. Whether the current legal framework governing forensic fingerprinting in India provides adequate and constitutionally sound safeguards to uphold the fundamental right to privacy in relation to the collection, storage and

use of biometric information?

The Indian legal framework governing forensic fingerprint collection in law and order is largely based on the Identification of Prisoners Act, 1920 and its modern-day replacement, the Criminal Procedure (Identification) Act, 2022[9]. The 2022 Act adds to the robustness and breadth of biometric data collection by allowing law enforcement agencies to collect palm prints, iris scans and other biological samples, in addition to fingerprints, from convicted individuals, arrested persons and certain categories of detainees.

However, the constitutionality of such expansive powers must be examined in the light of the right to privacy as recognized by the Supreme Court in Justice K. S. Puttaswamy (Retd.) v. Union of India[10]. In this seminal judgment, the Court recognized the right to privacy as a fundamental right protected under Article 21 of the Constitution. The Court also laid down the three-fold test of legality, necessity and proportionality, requiring that any state action that interferes with privacy must be backed by a valid law, pursue a legitimate state objective and adopt measures that are proportionate to that objective.

The 2022 Act meets the legal requirement by authorizing biometric collection statutorily. However, it has been criticized for failing to disclose the safeguards related to the storage, the duration of retention, and the lawful use of the biometric data collected under the Act. The Act provides for the National Crime Records Bureau to retain such data for a maximum period of seventy-five years, raising the concern of a disproportionate interference with personal privacy.

Additionally, India does not have a statutory framework governing the use of biometric data in criminal investigations akin to jurisdictions subjected to strict data protection regimes. While the Digital Personal Data Protection Act, 2023[11], provides a certain set of principles for the protection of personal data, it largely exempt government agencies for data processing performed for law enforcement purposes. This regulatory lacuna is evident in ensuring that the biometric data collected in the course of criminal investigations is safeguarded with sufficient privacy.

As a result, although current law allows forensic fingerprinting to be carried out, the lack of access control and restrictions on secondary use of biometric data in the present legal framework generates significant issues for the constitutional protection of proportionality and privacy.

2. Whether discretionary powers of law enforcement agencies in compulsory collection of fingerprints amount to an excessive violation of personal liberty, dignity and presumption of innocence particularly of undertrials and acquitted persons.

The Criminal Procedure (Identification) Act, 2022 empowers police officers and prison officials to collect various biometric measurements compulsorily from a wide range of persons including arrested persons and detainees. Section 3 of the Act empowers the police officers and prison officials to collect such measurements without the consent of the persons in various circumstances and therefore, the discretionary powers of police officers and prison officials in taking biometric measurements without the consent of the persons need to be examined to see whether it amounts to an excessive violation of personal liberty and dignity of the persons.

The Constitution guarantees the right to life and personal liberty under Article 21. The right to life and personal liberty includes human dignity and bodily integrity. The Supreme Court has consistently held that criminal procedure should be in line with the constitutional values. In Selvi v. State of Karnataka[12], the Court has noted that the involuntary undertaking of various techniques including narco-analysis, brain-mapping and polygraph test is a violation of the right against self-incrimination under Article 20(3) and an infringement of personal liberty. Fingerprint collection is a less intrusive

procedure than the above-mentioned techniques but the judgment in Selvi v State of Karnataka is significant in that it establishes a premise that investigative procedures cannot intrude upon the bodily autonomy of a person without adequate safeguards.

In the same vein, the state of Rajasthan v. Kashi Ram[13], in which the principle of presumption of innocence was upheld as a fundamental principle of criminal jurisprudence, the defendant should not be presumed as a criminal until the guilt has been established. Accordingly, compulsory collection of biometric information from undertrials, detainees and persons acquitted should not be taken, as such persons may compulsorily be in biometric databases for life even though they have not been convicted of any offence.

Accordingly, the powerful discretionary jurisdiction vested in law enforcement authorities will endanger the constitutional right of personal liberty, dignity and presumption of innocence on account of the long term retention of biometric information of non-convicted persons.

3. Absence of clear statutory norms on data retention, deletion and purpose limitation and oversight can create gaps for misuse, function creep and long-term surveillance of fingerprint databases.

One of the key concerns with India's forensic fingerprint regime is the lack of detailed statutory provisions on the entire lifecycle of data, including limits on data retention, deletion protocols and oversight mechanisms. The Criminal Procedure (Identification) Act, 2022 mandates that biometric records of individuals can be stored in centralized databases operated by the National Crime Records Bureau.

The Act does not specify when such data should be deleted, particularly for individuals who are acquitted, discharged or never actually charged with an offence. Though the law allows for courts to order destruction of records in certain circumstances, automatic deletion mechanisms and independent oversight bodies that monitor the management of database are not mandated.

Purpose limitation principle and fingerprint databases: An examination of the Indian constitutional standpoint. While ensuring privacy jurisprudence in India, one of the most important and important principles is that purpose limitation principle, which states that personal data collected for one purpose cannot be used for unrelated purposes without legal authority. In K. S. Puttaswamy (Retd.) v. Union of India, the Supreme Court of India stated that the state has to provide safeguards against any arbitrary surveillance and misuse of personal data.

In the absence of any rules regulating the retention period, deletion procedures and audit mechanisms, fingerprint databases may unintentionally grow beyond the scope of their investigative purpose. Such a "function creep" may turn criminal identification systems into instruments of population surveillance over time. This raises significant concerns about the compatibility of such usage with the democratic constitutional values.

4. How effective and adequate are current judicial approaches and procedural safeguards in the regulation of forensic fingerprinting practices, considering the development of privacy jurisprudence in India?

Indian courts have always noted the evidentiary value of fingerprints and, in doing so, have also been sensitive to issues of self-incrimination and procedural fairness. In State of Bombay v. Kathi Kalu Oghad[14], the Supreme Court noted that the compulsory collection of fingerprints, handwriting or physical measurements does not contravene Article 20(3) as such evidence is "physical evidence" and not "testimonial evidence". The Court, while reaffirming the legitimacy of such techniques as forensic evidence, also noted that such techniques should be done in accordance with procedural law, thus permitting investigative agencies to

collect fingerprints without violating the constitutional protection against self-incrimination.

However, the development of privacy jurisprudence and the recognition of privacy as a fundamental right in Justice K. S. Puttaswamy (Retd.) v. Union of India has led courts to re-examine older precedent in light of proportionality and data protection. While courts continue to admit evidence of fingerprints as reliable forensic evidence, there is still very limited jurisprudence on regulation of biometric databases, long-term storage and other issues.

Hence, while the judicial precedent acknowledges the legality of the evidence of fingerprints, the constitutional evolution points to a need for more extensive judicial examination of privacy and data protection concerns.

5. Whether India's current regime of forensic fingerprinting necessitates a rights-based regulatory framework that safeguards investigative efficiency while upholding obligations under both constitutional and human rights law.

In view of the rapid development of biometric technologies and centralized criminal databases, scholars increasingly contend that India's current legislation on forensic identification systems needs a rights-based regulatory framework that deals with the risks to privacy, accountability, transparency, and oversight. Existing legislation primarily deals with facilitating law enforcement agencies in collecting biometric measurements. According to international human rights norms, surveillance and biometric identification system are subject to stringent legal safeguards. Article 17 of International Covenant on Civil and Political Rights[15] bars arbitrary and unlawful interference in privacy. Biometric databases are increasingly subjected to regulation by independent supervisory authorities and data protection laws in democratic jurisdictions.

In India, although the Digital Personal Data Protection Act, 2023, brings in certain privacy norms, it does not specifically regulate biometric data collected in the course of criminal investigations. Therefore, the existing regime is largely governed by criminal procedure law rather than any specialized regulatory regime.

A rights-based regulatory regime would need statutory provisions on consent, data minimisation, limited retention, independent supervisory authorities and individuals' right to deletion. Thereby, law enforcement agencies can continue to use forensic fingerprinting while being in conformity with the constitutional guarantees provided under Articles 14, 19, 21 of the Constitution.

CASE REFERENCES:

(State of Bombay) v. Kathi Kalu Oghad[16] : AIR 1961 SC 1808

The Supreme Court decided whether the compulsory giving of fingerprints and specimen handwriting by an accused during criminal investigation violates Article 20(3) of the Constitution. The Court observed that fingerprints are a mere physical identification evidence and not a testimonial evidence, and their compulsory giving does not constitute self incrimination. The judgment confirmed that fingerprinting is permissible as an investigative technique; however, it should be confined within the limits of the law of criminal procedure.

Selvi v. State of Karnataka[17]: (2010) 7 SCC 263

The Supreme Court decided upon the constitutionality of investigative techniques such as narco-analysis and polygraph test. The Court ruled such investigative techniques un-constitutional as they impinge upon the mental privacy and personal liberty of an individual. However, the Court observed that these techniques are not permissible for the same reason that fingerprints are not permissible to be given during criminal investigation as they do not contain personal knowledge. The judgment thus clarified the boundary between forensic

physical identification and investigative techniques.

Justice K. S. Puttaswamy (Retd.) v. Union of India[18] (2017) 10 SCC 1

In the Extraordinary case, the Supreme Court recognized the right to privacy as an inherent fundamental right under Article 21. The Court further ruled that state collection of biometric identifiers like fingerprints is an interference with personal privacy and it is allowed only when it passes the constitutional tests of legality, necessity and proportionality. The judgment now paves the way for the constitutional standard regarding the laws which allow collection of fingerprints and biometric database for criminal investigations.

Ritesh Sinha v. State of Uttar Pradesh[19] (2019) 8 SCC 1

The Court dealt with the question whether an accused can be forced to give biometric identification evidence like voice sample during the course of a criminal investigation. The Supreme Court allowed such compulsion in the interest of justice but underlined that biometric evidence collection should be backed by statutory authority and also by constitutional safeguards. The Judgment stressed to me that investigative techniques that use biometric identification raise issues of privacy and personal liberty and hence must be conducted with caution.

D.K. Basu v. State of West Bengal[20]: (1997) 1 SCC 416

The Supreme Court laid down elaborate procedure to be followed by police in arrest and investigation to control abuse of power. The Court stressed that investigative procedure must be in conformance with human dignity and personal liberty guaranteed by Article 21. Even though fingerprinting is not specifically dealt with in this case, its principle is applicable to all investigative processes such as forensic identification processes like fingerprinting to be conducted with procedural safeguards and accountability.

CONCLUSION :

This paper analysed whether the legal framework of forensic fingerprinting in India balances the criminal investigation requirements and the constitutional right to privacy and freedom. Since forensic fingerprinting is considered one of the most scientifically reliable methods of identification in the criminal investigation, legal analysis of the body of law indicates that the legal framework of forensic fingerprinting does not address the substantial constitutional ramifications of collecting and storing biometric information.

Courts have endorsed the investigative utility of fingerprint evidence in criminal cases, by allowing it as admissible evidence in criminal trials, e.g., State of Bombay v. Kathi Kalu Oghad. However, the Supreme Court jurisprudence on the constitutional right to privacy has undergone significant change in recent years, with Justice K. S. Puttaswamy (Retd.) v. Union of India, and its progenies, extending the ambit of Article 21 right to privacy. This landmark case decided that the state cannot use biometric data unless it is lawful, necessary and proportionate. The legal framework of forensic identification does not reflect this safeguard[21].

The hypothesis advanced in this paper is thus well supported by the foregoing discussion. Forensic fingerprinting may continue to be a scientifically reliable and useful investigative tool, but it is necessary that in the Indian context the legal regulation of this activity be proportionate to the constitutional evolution of privacy and personal liberty. In the absence of appropriate safeguards and regulatory controls, the use of forensic fingerprinting has the potential to infringe personal liberty where it does not serve the interest of the state. A more robust legal framework for biometric identification will ensure that the use of forensic fingerprinting continues to serve the interests of criminal investigation while keeping in line with the constitutional guarantees of dignity, privacy and fundamental rights.

SUGGESTIONS:

1. Make provision for clear statutory safeguards on biometric data The legal framework for forensic fingerprinting should provide clear statutory safeguards on the collection, storage, access and use of biometric data. The law should define the situations which warrant the collection of fingerprints and also restrict the scope of use of the fingerprints to criminal investigations only. This would make sure that the statutory safeguards accord with the constitutional privacy standards set by Justice K. S. Puttaswamy (Retd.) v. Union of India.

2. Make provision for mandatory data retention and deletion The law should provide clear time limits on the retention of fingerprint records for those who were acquitted, discharged or not charged. The law should provide for an automatic mechanism for deletion of biometric data. This would reduce unwarranted surveillance and preserve the presumption of innocence in the criminal justice system.

3. Strengthen judicial oversight on biometric collection The compulsory collection of fingerprints on the course of criminal investigations should be subject to stronger judicial oversight, especially in ongoing investigations that involve individuals who are still not convicted. The magistrate should be called upon to examine and approve the collection of biometric data in sensitive cases, in order to make sure that the investigative powers are exercised in a proportionate manner, in conformity with the guarantees prescribed by the Constitution.

4. Create independent oversight structures for forensic databases An independent regulatory authority or oversight body should be created to oversee the management of the national fingerprint databases maintained by the investigative agencies. This authority should be tasked with monitoring the data access to these databases, ensuring that it is in conformity with privacy rules and investigating any misuse or unlawful disclosure of biometric data.

5. Train and provide ethical guidelines for the officers conducting investigations Investigating officers should be trained in forensic evidence collection and privacy protection. Explicit ethical guidelines will facilitate the collection of fingerprint evidence in a scientifically sound manner that respects constitutional rights and human dignity.

REFERENCES:

Statutes:

1. Criminal Procedure (Identification) Act, 2022
2. Code of Criminal Procedure, 1973
3. Information Technology Act, 2000
4. Digital Personal Data Protection Act, 2023
5. Indian Evidence Law Bibliography:

1. Galton, Francis. *Finger Prints*. London: Macmillan & Co., 1892.
2. Bhatia, Gautam. *Privacy in the Age of Surveillance: Constitutional Challenges in India*. New Delhi: Oxford University Press, 2016.
3. K. D. Gaur. *Textbook on Indian Penal Code*. 7th ed. New Delhi: Universal Law Publishing, 2020.
4. V. N. Shukla. *Constitution of India*. New Delhi: Eastern Book Company, 2021.

Webliography:

From-Fingerprints-to-Facial-Recognition.pdf

Forensic DNA Databanks and Privacy of Information - DNA Technology in Forensic Science

- NCBI Bookshelf

END NOTES

1 Bhatia, Gautam. Privacy in the Age of Surveillance: Constitutional Challenges in India. New Delhi: Oxford University Press, 2016.

2 Finger Prints is a book published by Francis Galton through Macmillan in 1892.

3 (2017) 10 SCC 1

4 AIR 1961 SC 1808; 1962 SCR (3) 10

5 William James Herschel is considered one of

the first Europeans to recognize the value of fingerprints for identification purposes

6 Galton, Francis. Finger Prints. London: Macmillan & Co., 1892

7 From-Fingerprints-to-Facial-Recognition.pdf

8 The National Automated Fingerprint Identification System (NAFIS) is a secure, web-based, pan-India database managed by the National Crime Records Bureau (NCRB) to digitize, store, and cross-match criminal fingerprints.

9 An Act to authorise for taking measurements of convicts and other persons for the purposes of identification and investigation in criminal matters and to preserve records and for matters connected therewith and incidental thereto

10 (2017) 10 SCC 1

11 THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 (NO. 22 OF 2023)

12 AIR 2010 SUPREME COURT 1974,

13 AIR 2007 SUPREME COURT 144,

14 (1962) 3 SCR 10

15 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

2. Everyone has the right to the protection of the law against such interference or attacks.

16 AIR 1961 SC 1808

17 (2010) 7 SCC 263

18 (2017) 10 SCC 1

19 (2019) 8 SCC 1

20 (1997) 1 SCC 416

21 V. N. Shukla. Constitution of India. New Delhi: Eastern Book Company, 2021.