VOLUME 6 | ISSUE 4

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

A SOCIO-LEGAL ANALYSIS OF BIOMETRIC DATA IN CRIMINAL INVESTIGATIONS

- S.K.Aruna Shankari[1]

ABSTRACT:

The rapid development of digital technologies and forensic science has transformed criminal investigations across the world. In India, biometric data such as fingerprints, iris scans, facial recognition data, voice samples, DNA profiling, and retinal scans have become important investigative tools used by law enforcement agencies[2]. The enactment of the Criminal Procedure (Identification) Act, 2022 has considerably expanded the powers of investigating authorities to collect, store, and process biometric information of accused persons, convicts, and detainees.[3] While biometric technologies enhance the efficiency of criminal justice administration, they also raise serious constitutional and human rights concerns relating to privacy, bodily autonomy, surveillance, misuse of data, and informational self-determination[4].This research critically examines the legal status of biometric data in criminal investigations in India. The study analyses constitutional safeguards under Articles 14, 20(3), and 21 of the Constitution of India, statutory provisions under the Criminal Procedure (Identification) Act, 2022, the Bharatiya Sakshya Adhiniyam, 2023, the Information Technology Act, 2000, and relevant judicial precedents.[5] The research further evaluates the admissibility and evidentiary value of biometric evidence in criminal proceedings. Comparative analysis with international frameworks such as the European Union's GDPR and United States forensic data practices is also undertaken[6].The study identifies significant gaps in Indian law relating to data protection safeguards, judicial oversight, proportionality

[1] Student and School of Excellence In Law, Tamilnadu Dr. Ambedkar Law University.
[2]Himanshu Mishra, *The Legal and Ethical Implications of Biometric and DNA Evidence in Criminal Law*, 12 **Indian Journal of Law & Technology** 44, 47 (2023).
[3]Criminal Procedure (Identification) Act, 2022, No. 11, Acts of Parliament, 2022 (India).
[4]*Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1.
[5]Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 (India).
[6]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1.

standards, retention periods, and accountability mechanisms[7]. It argues that the absence of a comprehensive legal framework governing biometric surveillance may lead to abuse of state power and violation of fundamental rights[8]. The paper concludes with recommendations for balancing national security and effective criminal investigation with constitutional liberties and privacy rights.

INTRODUCTION:

Biometric data refers to measurable biological and behavioural characteristics used for identifying individuals. Common forms of biometric data include fingerprints, iris patterns, retina scans, DNA samples, facial recognition records, voice patterns, and palm impressions.[9] In contemporary criminal investigations, biometric technologies have become essential instruments for identification of suspects, verification of criminal history, crime scene analysis, and forensic examination[10].India has witnessed rapid technological transformation in policing and criminal justice administration.[11] The increasing dependence on biometric identification systems such as Aadhaar, facial recognition technologies, and forensic databases has altered the nature of criminal investigations[12]. Traditionally, the Identification of Prisoners Act, 1920 permitted collection of fingerprints and photographs from convicted persons and certain arrested individuals.[13] However, the enactment of the Criminal Procedure (Identification) Act, 2022 considerably widened the scope of data collection by empowering law enforcement agencies to collect various "measurements," including fingerprints, palm impressions, footprints, photographs, iris and retina scans, signatures, handwriting, behavioural attributes, and biological samples[14]. The expanded powers of the State to collect and retain biometric information have generated constitutional concerns. The right to privacy recognized in Justice K.S. Puttaswamy v. Union of India established informational privacy as an intrinsic component of Article 21[15]. The collection of biometric data without adequate safeguards raises questions regarding proportionality, legality, consent, and procedural fairness[16].Moreover, biometric data possesses unique characteristics distinguishing it from

[7]DW News, *India's New Biometric Law Raises Privacy Concerns* (Apr. 2022)
[8]*Justice K.S. Puttaswamy (Retd.)*, (2017) 10 S.C.C. at 497.
[9]AZB & Partners, *Biometric Data Regulation in India: Legal Landscape and Risks* (2023).
[10]Ishan Sharma, *Forensic Evidence and Law in India* 78 (Eastern Book Co. 2022).
[11]Ministry of Home Affairs, Government of India, *Crime in India 2023 Statistics* (2023).
[12]Unique Identification Authority of India (UIDAI), *Aadhaar Authentication Framework* (2023).
[13]Identification of Prisoners Act, 1920, No. 33, Acts of Parliament, 1920 (India).
[14]Criminal Procedure (Identification) Act, 2022, § 2(b).
[15]*Justice K.S. Puttaswamy (Retd.)*, (2017) 10 S.C.C. 1, 497–98.
[16]Id.

ordinary personal information. Unlike passwords or identity numbers, biometric identifiers are permanent and cannot be altered if compromised[17]. Breaches involving biometric databases may expose individuals to lifelong risks of identity theft and surveillance.[18]This research analyses the legal status of biometric data in criminal investigations with special emphasis on constitutional protections, evidentiary admissibility, statutory frameworks, and privacy implications. The study adopts a doctrinal and socio-legal approach to critically examine whether existing Indian laws adequately balance effective criminal investigation with protection of civil liberties.

NEED FOR THE STUDY:

The present study is necessary for several reasons:

1. The increasing use of biometric technologies in criminal investigations has expanded State surveillance powers.
2. The Criminal Procedure (Identification) Act, 2022 significantly enlarges the scope of biometric data collection and retention.
3. India lacks a comprehensive and specialized statutory framework regulating biometric surveillance in criminal justice administration.
4. Judicial precedents relating to privacy, self-incrimination, and forensic evidence require critical analysis in the context of emerging technologies.
5. Concerns regarding misuse, data leaks, unauthorized access, and profiling have intensified due to several reported biometric breaches.
6. The study is important for understanding the evidentiary value and admissibility of biometric evidence under the Bharatiya Sakshya Adhiniyam, 2023.
7. There is a pressing need to evaluate whether current legal mechanisms comply with constitutional principles of proportionality and procedural fairness.
8. Comparative examination of international legal frameworks may assist in recommending reforms suitable for India.

SIGNIFICANCE OF THE STUDY:

The study possesses academic, legal, and social significance.

[17]AZB & Partners, supra note 8.
[18]Id.

1. **Academic Significance**

The research contributes to emerging scholarship on cyber law, digital evidence, privacy law, forensic science, and criminal justice administration.

2. Legal Significance

The study critically analyses constitutional provisions, statutory laws, and judicial precedents relating to biometric evidence and privacy rights.

3. Policy Significance

The research highlights legislative gaps and proposes reforms for establishing safeguards against misuse of biometric data.

4. **Social Significance**

The misuse of biometric information may result in surveillance, discrimination, wrongful arrests, identity theft, and violation of dignity. This study contributes to awareness regarding digital rights and data protection.

STATEMENT OF THE PROBLEM:

The increasing use of biometric technologies in criminal investigations has created tension between the State's interest in maintaining law and order and the individual's right to privacy and dignity. The Criminal Procedure (Identification) Act, 2022 empowers investigating agencies to collect and retain biometric information for extended periods without sufficient judicial oversight or data protection safeguards. The absence of comprehensive regulation regarding storage, sharing, retention, and destruction of biometric data creates possibilities for misuse, unauthorized surveillance, and constitutional violations. Therefore, the legal status and constitutional validity of biometric data collection and use in criminal investigations require critical examination.

RESEARCH GAP:

Existing studies primarily focus on either forensic science or privacy rights independently. Limited research comprehensively examines the intersection of biometric surveillance,

criminal investigations, constitutional rights, evidentiary admissibility, and data protection in the Indian legal context.

Further, there is insufficient doctrinal analysis regarding:

1. The compatibility of the Criminal Procedure (Identification) Act, 2022 with Article 21 privacy standards.
2. Judicial oversight mechanisms governing biometric data collection.
3. Retention and destruction policies for biometric databases.
4. Admissibility standards for biometric evidence under the Bharatiya Sakshya Adhiniyam, 2023.
5. Comparative evaluation between Indian law and international biometric governance frameworks.

This study seeks to bridge these gaps through a comprehensive socio-legal and doctrinal analysis.

RESEARCH QUESTIONS:

1. What is the legal status of biometric data in criminal investigations in India?
2. Whether the Criminal Procedure (Identification) Act, 2022 violates constitutional rights under Articles 14, 20(3), and 21?
3. What is the evidentiary value and admissibility of biometric evidence under Indian evidence law?
4. Whether existing legal safeguards sufficiently protect individuals against misuse of biometric data?
5. How do international legal frameworks regulate biometric surveillance and forensic databases?
6. What reforms are necessary to ensure balance between criminal investigation and privacy rights?

HYPOTHESIS:

1. The present legal framework governing biometric data in criminal investigations inadequately protects privacy and informational autonomy.

2. The Criminal Procedure (Identification) Act, 2022 grants excessive discretionary powers to investigating authorities without sufficient safeguards.
3. Existing Indian evidence laws are insufficient to address authenticity and chain-of-custody issues concerning biometric evidence.
4. A comprehensive data protection framework and judicial oversight mechanism are essential for constitutional compliance.

AIMS AND OBJECTIVES:

Aim

To critically analyse the legal status of biometric data in criminal investigations and evaluate its constitutional, evidentiary, and privacy implications.

Objectives

1. To examine the concept and types of biometric data.
2. To analyse statutory provisions governing biometric collection in India.
3. To study constitutional protections relating to privacy and self-incrimination.
4. To evaluate the admissibility and evidentiary value of biometric evidence.
5. To identify legal and procedural gaps in biometric data regulation.
6. To compare Indian legal mechanisms with international standards.
7. To recommend reforms ensuring accountability and data protection.

SCOPE OF THE STUDY:

The study focuses on biometric data used in criminal investigations within the Indian legal framework. It covers constitutional provisions, criminal procedure laws, evidence law, forensic science principles, and data protection issues. Comparative references are made to international legal systems wherever relevant.

LIMITATIONS OF THE STUDY:

1. The study is doctrinal in nature and relies mainly on secondary sources.
2. Rapid technological developments may render certain legal interpretations outdated.

3. Limited judicial precedents specifically addressing biometric surveillance are available.
4. The research does not include empirical fieldwork or interviews with law enforcement agencies.

RESEARCH METHODOLOGY:

The study adopts doctrinal and analytical research methodology. Primary sources include statutes, constitutional provisions, judicial decisions, government reports, and international legal instruments. Secondary sources include books, journal articles, research papers, reports, and online databases.

REVIEW OF LITERATURE:

1. Harsh Raj, Criminal Procedure (Identification) Act 2023: An Analysis from Evidence Law Perspective

The author critically analyses the Criminal Procedure (Identification) Act, 2022 and argues that the legislation lacks sufficient procedural safeguards regarding storage and handling of biometric evidence. The study highlights risks to privacy and evidentiary reliability arising from long-term digital storage.

2. Himanshu Mishra, The Legal and Ethical Implications of Biometric and DNA Evidence in Criminal Law

This article discusses constitutional concerns arising from biometric and DNA evidence, particularly privacy, self-incrimination, and ethical misuse of surveillance technologies.

3. AZB & Partners, Biometric Data Regulation in India: Legal Landscape and Risks

The paper analyses biometric risks in the Indian regulatory framework and emphasizes that biometric identifiers are permanent and highly vulnerable if compromised.

4. DW Report on India's Biometric Law

The report highlights criticism against the Criminal Procedure (Identification) Act, 2022 for granting extensive powers to police authorities to collect and store biometric information for seventy-five years.

5. Ishan Sharma, Forensic Evidence and Law in India

The author analyses the evidentiary status of forensic evidence including fingerprints and DNA profiling in Indian criminal trials.

CHAPTERISATION:

Chapter I – Introduction

- Concept of biometric data
- Nature and scope of criminal investigations
- Historical evolution of forensic identification

Chapter II – Legal Framework Governing Biometric Data

- Criminal Procedure (Identification) Act, 2022
- Bharatiya Nagarik Suraksha Sanhita, 2023
- Bharatiya Sakshya Adhiniyam, 2023
- Information Technology Act, 2000

Chapter III – Constitutional Dimensions

- Right to privacy
- Right against self-incrimination
- Due process and proportionality
- Surveillance jurisprudence

Chapter IV – Evidentiary Value of Biometric Data

- Admissibility of electronic evidence
- DNA and fingerprint evidence
- Chain of custody
- Reliability and forensic standards

Chapter VI – Comparative Analysis

Chapter V – Challenges and Concerns

- Data breaches
- Mass surveillance
- Facial recognition technologies
- Retention and misuse of biometric databases

Chapter VII – Recommendations and Suggestions

Chapter VIII – Conclusion

LEGAL FRAMEWORK GOVERNING BIOMETRIC DATA IN CRIMINAL INVESTIGATIONS :

Historically, the collection of biometric information was limited to fingerprints and photographs under the Identification of Prisoners Act, 1920[19]. However, technological advancements and evolving policing strategies led to the enactment of the Criminal Procedure (Identification) Act, 2022, which significantly widened the powers of law enforcement agencies to collect various forms of biometric data[20].The chapter critically examines statutory provisions governing biometric data in India, including the Criminal Procedure (Identification) Act, 2022, the Bharatiya Nagarik Suraksha Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023, the Information Technology Act, 2000, and relevant constitutional provisions. It also analyses judicial interpretations and concerns arising from unrestricted biometric surveillance.

Meaning of "Measurements" Under Indian Law

The Criminal Procedure (Identification) Act, 2022 introduced an expanded definition of "measurements." Section 2(b) defines measurements to include:

- Finger impressions
- Palm-print impressions
- Foot-print impressions

[19]Identification of Prisoners Act, 1920, No. 33, Acts of Parliament, 1920 (India).
[20]Criminal Procedure (Identification) Act, 2022, No. 11, Acts of Parliament, 2022 (India).

- Photographs
- Iris scans
- Retina scans
- Physical and biological samples
- Behavioural attributes
- Signatures
- Handwriting [21]

The inclusion of biological samples and behavioural characteristics considerably broadens the scope of biometric collection[22].Unlike the earlier Identification of Prisoners Act, 1920, the new legislation permits collection of technologically advanced biometric identifiers, thereby enabling the State to establish extensive biometric databases.

Identification of Prisoners Act, 1920

Historical Background :

The Identification of Prisoners Act, 1920 was enacted during the colonial period to facilitate criminal identification through fingerprints and photographs.[23]The legislation empowered police authorities to obtain fingerprints and photographs of convicted persons and certain arrested individuals.[24]

The Act mainly focused on:

- Fingerprints
- Footprints
- Photographs

At the time of enactment, advanced biometric technologies such as DNA profiling and facial recognition did not exist.

Scope of the Act :

[21]Id. § 2(b).
[22]Harsh Raj, *Criminal Procedure (Identification) Act, 2022: An Analysis from an Evidence Law Perspective*, 8 **National Law Review** 91, 96 (2023).
[23]Identification of Prisoners Act, 1920, No. 33, Acts of Parliament, 1920 (India).
[24]Id. §§ 3–5.

The 1920 Act authorized:

1. Collection of measurements from convicted persons.
2. Collection from arrested individuals in specified cases.
3. Magistrates to order collection where necessary for investigation.

The law was relatively narrow in scope and primarily intended for identification purposes.

Limitations of the 1920 Act :

The major limitations included[25]:

- No provision for DNA profiling.
- No recognition of digital biometric systems.
- Absence of centralized biometric databases.
- Limited categories of persons covered.
- Lack of technological adaptability.

Due to these shortcomings, the government introduced the Criminal Procedure (Identification) Act, 2022.

Criminal Procedure (Identification) Act, 2022 :

The Criminal Procedure (Identification) Act, 2022 replaced the Identification of Prisoners Act, 1920[26].The legislation substantially expanded police powers relating to collection and retention of biometric data.[27]

The Act aims to:

- Modernize criminal investigation procedures.
- Improve conviction rates.
- Facilitate digital identification systems.
- Create centralized criminal databases.

[25]Harsh Raj, supra note 21, at 97.
[26]Criminal Procedure (Identification) Act, 2022, No. 11, Acts of Parliament, 2022 (India).
[27]Id.

However, the legislation has generated widespread constitutional debate due to concerns regarding privacy, surveillance, and abuse of power.

Persons Covered Under the Act :

The Act permits collection of measurements from:

1. Convicted persons.
2. Persons ordered to give security for good behaviour.
3. Arrested individuals.
4. Preventive detainees.
5. Persons detained under preventive detention laws.

Section 3 allows even persons arrested for minor offences to be subjected to biometric collection under certain circumstances[28].This significantly enlarges State power compared to the earlier law.

Powers of Police and Magistrates :

The legislation authorizes:

- Police officers,
- Prison officers, and
- Magistrates

to direct individuals to provide biometric measurements.A Magistrate may compel a person to provide measurements if considered necessary for investigation or prosecution.

Collection of Biological Samples :

One of the most controversial aspects of the Act is authorization to collect "biological samples[29]," which may include:

- Blood
- Saliva

[28]Id. § 3.
[29]Id. § 2(b).

- Hair
- Semen
- DNA material

Collection of such samples directly affects bodily integrity and raises constitutional concerns under Articles 20(3) and 21.

Retention and Storage of Data :

The Act permits retention of biometric records for seventy-five years.The National Crime Records Bureau (NCRB) is empowered to[30]:

- Store records,
- Process biometric information,
- Share records with law enforcement agencies,
- Destroy records in specified circumstances.

Critics argue that seventy-five-year retention amounts to virtual lifetime surveillance.

Resistance to Collection :

Section 6 provides that resistance or refusal to provide measurements shall be deemed an offence under Section 186 of the Bharatiya Nyaya Sanhita (formerly IPC § 186).

This provision effectively criminalizes non-cooperation.

Constitutional Challenges to the 2022 Act :

The constitutionality of the Criminal Procedure (Identification) Act, 2022 has been challenged before courts on several grounds.

A. Violation of Right to Privacy

The right to privacy recognized in Justice K.S. Puttaswamy v. Union of India protects informational autonomy and bodily integrity.[5]

Mandatory biometric collection without safeguards may violate:

[30]Id. § 4.

- Personal liberty,
- Informational privacy,
- Human dignity.

B. Excessive Delegation of Power

Critics argue that the legislation grants wide discretionary powers to police authorities without:

- Judicial oversight,
- Independent supervision,
- Accountability mechanisms.

C. Proportionality Concerns

The Supreme Court in Puttaswamy established the proportionality test requiring:

1. Legality,
2. Legitimate aim,
3. Necessity,
4. Procedural safeguards.

The indefinite collection and storage of biometric information may fail this test.

D. Presumption of Innocence

Collection of biometric data from persons merely arrested and not convicted undermines the principle of presumption of innocence.

Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) :

The Bharatiya Nagarik Suraksha Sanhita, 2023 replaced the Code of Criminal Procedure, 1973 and contains procedural provisions relating to investigation and evidence collection.

Medical Examination of Accused :

The BNSS permits medical examination of accused persons where necessary for investigation.

This includes:

- Blood samples,
- DNA collection,
- Bodily examinations.

Search and Seizure of Electronic Evidence :

Digital biometric evidence stored in:

- Mobile phones,
- Laptops,
- CCTV systems,
- Cloud servers

may be seized during investigation.

Scientific Investigation :The BNSS encourages use of forensic science and scientific methods in criminal investigation, especially for offences punishable with seven years or more.This strengthens reliance on biometric technologies.

Bharatiya Sakshya Adhiniyam, 2023 :

The Bharatiya Sakshya Adhiniyam, 2023 replaced the Indian Evidence Act, 1872 and governs admissibility of biometric evidence.

Electronic Evidence :

Biometric records stored electronically are treated as electronic evidence.Sections 63 and 65 establish conditions regarding:

- Authenticity,
- Integrity,
- Certification,
- Reliability.

Admissibility of DNA and Fingerprint Evidence

Courts increasingly rely upon:

- DNA profiling,
- Fingerprints,
- Voice samples,
- Digital facial recognition evidence.

However, evidentiary reliability depends on:

- Proper forensic procedure,
- Chain of custody,
- Scientific accuracy.

Expert Evidence : Expert testimony from forensic scientists is admissible under provisions relating to expert opinion.Courts rely heavily upon forensic experts in biometric identification cases.

Information Technology Act, 2000 :

The Information Technology Act, 2000 contains provisions indirectly relevant to biometric protection.

Section 43A :

Body corporates handling sensitive personal data must maintain reasonable security practices.

Biometric data falls within sensitive personal information.

SPDI Rules, 2011 :

The Sensitive Personal Data or Information Rules classify:

- Fingerprints,
- DNA,
- Physiological data

as sensitive personal data requiring protection.

Digital Personal Data Protection Act, 2023:

The Digital Personal Data Protection Act, 2023 establishes a framework for protection of digital personal data.

Although law enforcement agencies may receive exemptions, the legislation highlights principles such as:

- Purpose limitation,
- Data minimization,
- Accountability,
- Consent.

However, broad State exemptions weaken privacy safeguards.

Judicial Decisions on Biometric Evidence :

Ritesh Sinha v. State of Uttar Pradesh

The Supreme Court permitted compulsory voice samples during investigation.The Court observed that technological advancement requires flexible interpretation of criminal procedure laws.

Justice K.S. Puttaswamy v. Union of India

This landmark judgment recognized privacy as a fundamental right and established the proportionality doctrine.The ruling has become central to challenges against biometric surveillance laws.

Role of National Crime Records Bureau (NCRB):

The NCRB functions as the central repository for biometric records.

Its responsibilities include:

- Collection,
- Processing,
- Preservation,

- Sharing of biometric information.

The centralized database increases efficiency but also creates risks relating to:

- Cyberattacks,
- Unauthorized access,
- Data misuse.

CONSTITUTIONAL DIMENSIONS OF BIOMETRIC DATA IN CRIMINAL INVESTIGATIONS :

Article 21 and Right to Privacy :

Scope of Article 21 :

Article 21 of the Constitution states:"No person shall be deprived of his life or personal liberty except according to procedure established by law.[31]"Initially, Article 21 was interpreted narrowly in *A.K. Gopalan v. State of Madras*.However, subsequent judicial interpretation expanded its scope significantly. In *Maneka Gandhi v. Union of India*[32], the Supreme Court held that any procedure depriving personal liberty must be:

- Fair,
- Just, and
- Reasonable.

This interpretation transformed Article 21 into a repository of several derivative rights including:

- Right to privacy,
- Right to dignity,
- Right to bodily autonomy,
- Right to informational self-determination.

Biometric collection directly implicates these rights because it involves extraction and processing of deeply personal biological information.In Justice K.S. Puttaswamy v. Union of IndiaThe landmark judgment in *Justice K.S. Puttaswamy v. Union of India* recognized

[31]INDIA CONST. art. 21.
[32]*Maneka Gandhi v. Union of India*, (1978) 1 S.C.C. 248.

privacy as a fundamental right protected under Part III of the Constitution[33].The case arose in the context of Aadhaar and biometric identity collection by the government. A nine-judge bench unanimously held that privacy is intrinsic to:

- Life,
- Liberty,
- Human dignity.

The Court observed:"Privacy includes at its core the preservation of personal intimacies, the sanctity of family life, marriage, procreation, the home and sexual orientation."The judgment recognized multiple dimensions of privacy:

1. Physical privacy
2. Informational privacy
3. Decisional autonomy

Biometric information falls within informational privacy because it involves personal data capable of identifying an individual permanently[34].

Informational Privacy :

The Court in *Puttaswamy* emphasized that informational privacy allows individuals to control dissemination and use of personal data.Biometric information is highly sensitive becaus[35]e:

- It is unique,
- Permanent,
- Irreplaceable,
- Difficult to anonymize.

Unlike passwords or identification cards, biometric identifiers cannot be changed if compromised. Therefore, unauthorized access to biometric databases creates long-term risks of identity theft and surveillance.[36]The Court acknowledged dangers associated with:

- State surveillance,

[33]*Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1.
[34]Id. at 497.
[35]Id.
[36]AZB & Partners, supra note 8.

- Data aggregation,
- Profiling,
- Behavioural monitoring.

These concerns become especially relevant in criminal investigations involving centralized biometric databases maintained by law enforcement agencies.

Proportionality Doctrine

Test of Proportionality :The Supreme Court in *Puttaswamy* established that any restriction on privacy must satisfy the proportionality test.The four-fold test includes[37]:

1. Legality
2. Legitimate State Aim
3. Necessity
4. Procedural Safeguards

A. Legality

There must exist a valid law authorizing biometric collection.

B. Legitimate Aim

The objective must relate to legitimate State interests such as:

- Crime prevention,
- National security,
- Public order.

C. Necessity

The measure adopted must be necessary and minimally intrusive.

D. Procedural Safeguards

Adequate safeguards must exist against abuse.

[37] *Justice K.S. Puttaswamy (Retd.),* (2017) 10 S.C.C. at 325–26.

The Criminal Procedure (Identification) Act, 2022 has been criticized for failing to satisfy proportionality because it permits broad biometric collection without sufficient safeguards[38].

Right Against Self-Incrimination Under Article 20(3) :

Article 20(3) provides:"No person accused of any offence shall be compelled to be a witness against himself[39]."This provision protects individuals from testimonial compulsion and coerced confessions.The constitutional issue in biometric collection is whether compelled extraction of fingerprints, DNA, voice samples, and biological material amounts to self-incrimination.

State of Bombay v. Kathi Kalu Oghad[40]

The Supreme Court held that fingerprints and handwriting samples are not testimonial compulsion under Article 20(3).The Court distinguished between:

- Physical evidence, and
- Testimonial evidence.

Selvi v. State of Karnataka[41]

The Court held that narco-analysis, polygraph tests, and brain-mapping conducted without consent violate Article 20(3).

The judgment emphasized:

- Mental privacy,
- Bodily integrity,
- Human dignity.

Article 14 and Equality Before Law :

Arbitrariness Doctrine :

[38]Harsh Raj, supra note 21, at 101.
[39]INDIA CONST. art. 20, cl. 3.
[40]*State of Bombay v. Kathi Kalu Oghad*, A.I.R. 1961 S.C. 1808.
[41]*Selvi v. State of Karnataka*, (2010) 7 S.C.C. 263.

Article 14 guarantees equality before law and prohibits arbitrary State action.The Supreme Court has repeatedly held that arbitrariness violates Article 14.Biometric surveillance systems may violate equality principles due to:

- Selective targeting,
- Discriminatory profiling,
- Algorithmic bias.

Facial Recognition and Discrimination : Facial recognition systems have been criticized for:

- Racial bias,
- Gender inaccuracies,
- Misidentification of minorities.

Absence of transparency in algorithmic decision-making may lead to unconstitutional discrimination.Biometric technologies significantly enhance surveillance capacity.In PUCL v. Union of India,the Supreme Court recognized telephone tapping as an invasion of privacy.The Court emphasized procedural safeguards against arbitrary surveillance.This principle equally applies to biometric monitoring systems.

DNA Profiling and Constitutional Concerns :

DNA contains highly sensitive genetic information revealing:

- Identity,
- Family lineage,
- Medical predispositions.

Therefore, DNA databases raise unique privacy concerns.

Privacy Risks in DNA Databases :

Risks associated with DNA databases include:

1. Genetic discrimination
2. Familial surveillance
3. Data misuse

4. Unauthorized sharing

Retention of DNA information for seventy-five years may amount to disproportionate surveillance.

International Constitutional Perspectives :

European Court of Human Rights

In S. and Marper v. United Kingdom, the European Court of Human Rights held that indefinite retention of fingerprints and DNA records of innocent persons violates the right to privacy under Article 8 of the European Convention on Human Rights.The Court emphasized proportionality and necessity.

United States

In Maryland v. King, the U.S. Supreme Court upheld DNA collection from arrested persons, considering it a legitimate identification procedure.However, dissenting judges warned against expansion of genetic surveillance.

EVIDENTIARY VALUE OF BIOMETRIC DATA IN CRIMINAL INVESTIGATIONS :

Meaning and Nature of Biometric Evidence :

Biometric evidence refers to identification evidence derived from unique biological or behavioural characteristics of individuals[42]. Such evidence is used to establish identity or association between a suspect and criminal activity.

Biometric evidence possesses the following characteristics[43]:

1. Scientific nature
2. Uniqueness
3. Permanence
4. Measurability

[42]Ishan Sharma, supra note 9, at 85.
[43]Id

5. Reliability

Unlike circumstantial evidence or eyewitness testimony, biometric evidence is often regarded as highly objective because it is based on scientific analysis rather than human perception.

Types of Biometric Evidence :

Fingerprint Evidence

Fingerprint evidence is one of the oldest and most widely accepted forms of biometric identification.[44]

A. Scientific Basis

Fingerprints consist of unique ridge patterns found on human fingers. The principle underlying fingerprint science is that:

- No two individuals possess identical fingerprints,
- Fingerprint patterns remain unchanged throughout life.

B. Evidentiary Importance

Fingerprint evidence assists in:

- Identifying accused persons,
- Connecting suspects to crime scenes,
- Detecting repeat offenders.

Latent fingerprints recovered from crime scenes are compared with known samples using forensic techniques.

C. Judicial Recognition

Indian courts have consistently recognized fingerprint evidence as admissible and reliable[45].In *State of Uttar Pradesh v. Ram Babu Misra*, the Supreme Court held that courts

[44]*State of Uttar Pradesh v. Ram Babu Misra*, (1980) 2 S.C.C. 343.
[45]Id

may direct accused persons to provide specimen signatures and fingerprints for investigation purposes.[46]

DNA Profiling :

Meaning of DNA Evidence :

DNA (Deoxyribonucleic Acid) contains genetic information unique to every individual except identical twins.

DNA samples may be extracted from:

- Blood,
- Hair,
- Saliva,
- Skin tissues,
- Semen,
- Bone fragments.

Evidentiary Significance :

DNA evidence is particularly important in[47]:

- Murder cases,
- Sexual offences,
- Paternity disputes,
- Missing person identification,
- Disaster victim identification.

[46]Id

[47]*Mukesh v. State (NCT of Delhi)*, (2017) 6 S.C.C. 1.

Judicial Recognition of DNA Evidence :

Indian courts have increasingly relied upon DNA evidence in criminal adjudication.*In Mukesh v. State (NCT of Delhi)*[48] , In the Nirbhaya case, DNA evidence played a crucial role in linking the accused with the crime.The Court accepted forensic biological evidence as highly reliable due to proper scientific analysis and chain of custody.

Voice Sample Evidence :

Voice recognition technology is increasingly used in:

- Cybercrime investigations,
- Terrorism cases,
- Telecommunication offences.

Voice spectrography compares sound wave patterns to identify speakers.

Judicial Position :

In Ritesh Sinha v. State of Uttar Pradesh ,The Supreme Court held that courts possess authority to compel accused persons to provide voice samples during investigation.

The Court observed that:

- Voice samples constitute physical evidence,
- They do not violate Article 20(3).

The judgment expanded investigative powers relating to biometric evidence.[49]

Facial Recognition Evidence :

Facial recognition systems use algorithms to compare facial features with stored databases.

Uses:

- Crowd surveillance,
- Identification of suspects,

[48]Id
[49]*Ritesh Sinha v. State of Uttar Pradesh*, (2019) 8 S.C.C. 1.

- Monitoring protests,
- Tracking fugitives.

Iris and Retina Scan Evidence :

Iris and retina scans identify unique eye patterns.These technologies are:

- Highly accurate,
- Difficult to forge,
- Increasingly used in digital authentication systems.

However, use in criminal investigations remains relatively limited compared to fingerprints and DNA.

Admissibility of Biometric Evidence Under Indian Law

Bharatiya Sakshya Adhiniyam, 2023 :

The Bharatiya Sakshya Adhiniyam, 2023 replaced the Indian Evidence Act, 1872 and governs admissibility of electronic and scientific evidence.Biometric records stored digitally qualify as electronic evidence.

Scientific evidence becomes relevant when it assists courts in:

- Establishing identity,
- Confirming presence at crime scenes,
- Corroborating prosecution narratives.

Expert testimony plays a crucial role in interpreting forensic findings.

Expert Opinion:

Forensic experts provide opinions regarding:

- DNA analysis,
- Fingerprint comparison,
- Voice identification,
- Biometric matching.

Courts generally treat expert opinion as corroborative evidence rather than conclusive proof.

Judicial Approach :

In Ram Chandra v. State of Uttar Pradesh ,The Supreme Court held that expert evidence must be carefully evaluated because expert opinion is advisory in nature.

Electronic Nature of Biometric Records :

Modern biometric systems store information electronically.Examples include:

- Fingerprint databases,
- DNA repositories,
- Facial recognition software,
- CCTV-integrated biometric systems.

Electronic biometric evidence must satisfy authenticity and integrity requirements.

Section 65B and Electronic Evidence :

Under the earlier Indian Evidence Act, Section 65B governed admissibility of electronic records[50].The Bharatiya Sakshya Adhiniyam similarly requires:

- Certification,
- Authenticity,
- Proper electronic handling.

In the case Anvar P.V. v. P.K. Basheer ,The Supreme Court held that electronic evidence is admissible only upon compliance with certification requirements.The judgment emphasized:

- Integrity of electronic systems,
- Reliability of digital records. [51]

This principle applies equally to biometric databases and digital forensic records.

[50]Bharatiya Sakshya Adhiniyam, 2023, §§ 63–65.
[51]*Anvar P.V. v. P.K. Basheer*,(2014) 10 S.C.C. 473.

Chain of Custody

Meaning :

Chain of custody refers to documented handling of evidence from:

- Collection,
- Preservation,
- Transportation,
- Analysis,
- Presentation before court.

Importance :

Proper chain of custody ensures:

1. Authenticity
2. Reliability
3. Prevention of tampering
4. Evidentiary integrity

COMPARATIVE ANALYSIS OF BIOMETRIC DATA REGULATION IN CRIMINAL INVESTIGATIONS: INDIA AND OTHER COUNTRIES

United States :

Legal Framework

The United States extensively uses biometric technologies in:

- Criminal investigations,
- Border control,
- Counterterrorism.

Key legal protections arise under:

- Fourth Amendment,
- Federal privacy laws,
- State biometric statutes.

Biometric systems used include:

- FBI's Integrated Automated Fingerprint Identification System (IAFIS),
- Combined DNA Index System (CODIS),
- Facial recognition databases.

Fourth Amendment Protection

The Fourth Amendment protects against unreasonable searches and seizures.

Courts evaluate biometric collection based on:

- Reasonableness,
- Probable cause,
- Warrants.

In *Maryland v. King*[52], the U.S. Supreme Court upheld collection of DNA samples from arrested individuals charged with serious offences.The Court held:

- DNA collection is similar to fingerprinting,
- It serves legitimate identification purposes.

However, dissenting judges warned that unrestricted DNA collection may enable mass genetic surveillance[53].

State Biometric Privacy Laws

Certain states provide stronger protections.Illinois Biometric Information Privacy Act (BIPA)Illinois enacted one of the strongest biometric privacy laws globally.BIPA requires:

- Informed consent,
- Data protection measures,
- Purpose limitation,
- Right to sue for violations.

The law has been used against corporations misusing facial recognition data.

[52]*Maryland v. King*, 569 U.S. 435 (2013).
[53]Id. at 482 (Scalia, J., dissenting).

United Kingdom :

Legal Framework

The United Kingdom regulates biometric information through:

- Protection of Freedoms Act, 2012,
- Data Protection Act, 2018,
- Human Rights Act, 1998.

Police authorities maintain:

- DNA databases,
- Fingerprint repositories,
- Facial recognition systems.

In *S. and Marper v. United Kingdom*[54], the European Court of Human Rights held that indefinite retention of DNA and fingerprints of innocent persons violated Article 8 of the European Convention on Human Rights.

The Court emphasized:

- Privacy,
- Human dignity,
- Proportionality.

Following this judgment, the UK modified its retention policies.

Protection of Freedoms Act, 2012

The Act introduced safeguards such as:

- Limited retention periods,
- Destruction of innocent persons' biometric data,
- Independent oversight mechanisms.

[54]*S. & Marper v. United Kingdom*, 2008-V Eur. Ct. H.R. 213.

Facial Recognition Concerns

The UK has increasingly used live facial recognition technology in public surveillance.IN R (Bridges) v. South Wales Police,The Court of Appeal held that police use of facial recognition lacked sufficient safeguards and violated privacy protections.

The judgment emphasized:

- Transparency,
- Accountability,
- Human rights compliance.

European Union :

GDPR and Biometric Data

The European Union provides one of the world's strongest privacy protection frameworks through the General Data Protection Regulation (GDPR).Under GDPR:

- Biometric data is classified as "special category data[55]."
- Processing requires strict legal justification.

Principles Governing Biometric Processing

The GDPR imposes:

1. Data minimization
2. Purpose limitation
3. Transparency
4. Accountability
5. Storage limitation
6. Explicit consent

Law Enforcement Directive

Biometric processing by police agencies must satisfy[56]:

[55]Regulation (EU) 2016/679, art. 9

- Necessity,
- Proportionality,
- Human rights compliance.

Independent supervisory authorities oversee data protection.

China :

Expansion of State Surveillance

China operates one of the world's largest biometric surveillance systems.

Technologies include:

- Facial recognition,
- DNA databases,
- AI-powered surveillance,
- Mass CCTV monitoring.

Legal Framework

China enacted:

- Personal Information Protection Law (PIPL),
- Cybersecurity Law.

However, State security interests often override privacy protections.

Facial Recognition and Public Monitoring

Facial recognition is extensively used for:

- Public surveillance,
- Social control,
- Monitoring ethnic minorities.

[56]Id

Canada :

Legal Framework

Canada regulates biometric data through:

- Privacy Act,
- Personal Information Protection and Electronic Documents Act (PIPEDA),
- Canadian Charter of Rights and Freedoms.

Constitutional Protections

The Canadian Charter protects:

- Privacy,
- Liberty,
- Protection against unreasonable search and seizure.

Courts apply proportionality analysis before approving intrusive surveillance measures.

Country	**Privacy Protection**	**Retention Policy**	**Judicial Oversight**	**Facial Recognition Regulation**
India	Moderate	75 years	Limited	Weak
United States	Moderate	Variable	Strong	Mixed
United Kingdom	Strong	Limited retention	Strong	Regulated
European Union	Very Strong	Restricted	Strong	Strict safeguards
China	Weak	Extensive	Minimal	Mass surveillance
Canada	Strong	Controlled	Strong	Privacy-focused

CHALLENGES RELATING TO BIOMETRIC DATA IN CRIMINAL INVESTIGATIONS :

1. Violation of Privacy

Biometric data such as fingerprints, DNA profiles, iris scans, and facial recognition records contain highly sensitive personal information. Excessive collection and storage of such data may violate the right to privacy under Article 21 of the Constitution.

In Justice K.S. Puttaswamy v. Union of India, the Supreme Court recognized privacy as a fundamental right.

2. Mass Surveillance

Facial recognition systems and biometric databases enable continuous monitoring of citizens. Excessive State surveillance may restrict freedom of speech, movement, and democratic participation.

3. Lack of Comprehensive Data Protection Law

India lacks a specialized law exclusively regulating biometric data in criminal investigations. Existing safeguards are inadequate regarding:

- Data retention,
- Data sharing,
- Deletion mechanisms,
- Independent oversight.

4. Indefinite Retention of Data

The Criminal Procedure (Identification) Act, 2022 permits retention of biometric records for seventy-five years. This may result in lifetime surveillance even for persons who are acquitted.

5. Cybersecurity Risks and Data Breaches

Biometric databases are vulnerable to:

- Hacking,
- Cyberattacks,
- Unauthorized access,
- Identity theft.

Unlike passwords, biometric information cannot be changed once compromised.

6. Wrongful Identification

Biometric systems, especially facial recognition technologies, may produce false matches due to:

- Poor image quality,
- Algorithmic errors,
- Human mistakes.

This may lead to wrongful arrests and miscarriage of justice.

7. Algorithmic Bias and Discrimination

Facial recognition technologies may disproportionately affect minorities, women, and marginalized communities due to biased datasets and inaccurate algorithms.

8. Constitutional Concerns

Compulsory extraction of biometric samples may violate:

- Article 20(3) – Right against self-incrimination,
- Article 21 – Right to dignity and bodily integrity.

In Selvi v. State of Karnataka, the Supreme Court emphasized protection of mental privacy and bodily autonomy.

9. Lack of Judicial Oversight

Biometric collection often occurs without prior judicial authorization, increasing possibilities of misuse and arbitrary police action.

10. Ethical Concerns

Use of biometric technologies raises ethical issues relating to:

- Consent,

- Human dignity,
- Bodily autonomy,
- State control over personal identity.

SUGGESTIONS :

1. Enact Comprehensive Biometric Data Protection Law

India should introduce a separate legislation specifically regulating collection, storage, use, sharing, and destruction of biometric data in criminal investigations.

2. Strengthen Judicial Oversight

Collection of sensitive biometric information such as DNA and retina scans should require prior judicial authorization to prevent arbitrary police action.

3. Limit Data Retention Period

Biometric records should not be retained for excessive periods. Data of acquitted persons should be deleted within a reasonable time.

4. Establish Independent Supervisory Authority

An independent regulatory body should monitor biometric databases and ensure accountability, transparency, and compliance with privacy standards.

5. Improve Cybersecurity Measures

Government agencies should adopt strong encryption and cybersecurity systems to prevent hacking, data breaches, and unauthorized access.

6. Regulate Facial Recognition Technology

Specific guidelines and legislation should govern use of facial recognition systems to prevent mass surveillance and discriminatory profiling.

7. Ensure Transparency and Accountability

Citizens should be informed about:

* Purpose of data collection,

* Storage duration,

* Rights relating to correction and deletion of data

8. Adopt International Best Practices

India may adopt privacy safeguards similar to the GDPR framework followed in the European Unio

9. Provide Training to Investigating Agencies

Police and forensic officers should receive proper training regarding ethical handling and scientific collection of biometric evidence.

10. Protect Fundamental Rights

All biometric collection procedures must comply with constitutional protections under Articles 14, 20(3), and 21 of the Constitution of India.

CONCLUSION :

Biometric technologies have transformed modern criminal investigations by enhancing identification accuracy and forensic efficiency. However, the extensive collection, storage, and processing of biometric data raise profound constitutional, ethical, and legal concerns. The Criminal Procedure (Identification) Act, 2022 significantly expands investigative powers without corresponding safeguards relating to privacy, oversight, and accountability.The right to privacy recognized under Article 21 requires that any restriction must satisfy legality, necessity, and proportionality. While biometric evidence may strengthen criminal justice administration, unrestricted surveillance and indefinite retention threaten democratic freedoms and civil liberties.India must therefore develop a balanced legal framework that protects both national security interests and constitutional rights. Strong data protection laws, judicial oversight, transparency mechanisms, and accountability standards are essential for ensuring lawful and ethical use of biometric technologies in criminal investigations.

REFERENCES :

TABLE OF CASES :

1. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
2. Maneka Gandhi v. Union of India, (1978) 1 S.C.C. 248 (India).
3. State of Bombay v. Kathi Kalu Oghad, A.I.R. 1961 S.C. 1808 (India).
4. Selvi v. State of Karnataka, (2010) 7 S.C.C. 263 (India).

5. Ritesh Sinha v. State of Uttar Pradesh, (2019) 8 S.C.C. 1 (India).
6. State of Uttar Pradesh v. Ram Babu Misra, (1980) 2 S.C.C. 343 (India).
7. Mukesh v. State (NCT of Delhi), (2017) 6 S.C.C. 1 (India).
8. Anvar P.V. v. P.K. Basheer, (2014) 10 S.C.C. 473 (India).
9. PUCL v. Union of India, (1997) 1 S.C.C. 301 (India).
10. Maryland v. King, 569 U.S. 435 (2013).
11. S. & Marper v. United Kingdom, 2008-V Eur. Ct. H.R. 213.
12. R (Bridges) v. South Wales Police, [2020] EWCA Civ 1058.
13. A.K. Gopalan v. State of Madras, A.I.R. 1950 S.C. 27 (India).

STATUTES AND LEGISLATIONS :

India

1. INDIA CONST. arts. 14, 20(3), 21.
2. Criminal Procedure (Identification) Act, 2022, No. 11, Acts of Parliament, 2022 (India).
3. Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46, Acts of Parliament, 2023 (India).
4. Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 (India).
5. Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
6. Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
7. Identification of Prisoners Act, 1920, No. 33, Acts of Parliament, 1920 (India).
8. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E), Gazette of India, Extraordinary, pt. II, sec. 3(i) (Apr. 11, 2011).

International Instruments :

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1.
2. Protection of Freedoms Act 2012, c. 9 (UK).
3. Data Protection Act 2018, c. 12 (UK).
4. Human Rights Act 1998, c. 42 (UK).
5. Personal Information Protection Law of the People's Republic of China (2021).

6. Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 (Can.).

BOOKS :

1. ISHAN SHARMA, FORENSIC EVIDENCE AND LAW IN INDIA (Eastern Book Co. 2022).
2. AVTAR SINGH & HARPREET KAUR, INTRODUCTION TO FORENSIC SCIENCE IN CRIMINAL INVESTIGATION (LexisNexis 2021).
3. V.D. MAHAJAN, CONSTITUTIONAL LAW OF INDIA (Eastern Book Co. 2023).
4. RATANLAL & DHIRAJLAL, THE LAW OF EVIDENCE (LexisNexis 2022).
5. CYRIL H. WECHT & JOHN T. RAGO, FORENSIC SCIENCE AND LAW: INVESTIGATIVE APPLICATIONS IN CRIMINAL, CIVIL, AND FAMILY JUSTICE (CRC Press 2019).

JOURNAL ARTICLES :

1. Himanshu Mishra, The Legal and Ethical Implications of Biometric and DNA Evidence in Criminal Law, 12 Indian J. L. & Tech. 44 (2023).
2. Harsh Raj, Criminal Procedure (Identification) Act, 2022: An Analysis from an Evidence Law Perspective, 8 Nat'l L. Rev. 91 (2023).
3. Apar Gupta & Kritika Bansal, Surveillance and Privacy in India: Constitutional Challenges of Biometric Governance, 5 Indian L. Rev. 77 (2022).
4. Anirudh Burman, Data Protection and Informational Privacy in India, 14 NUJS L. Rev. 112 (2021).
5. Usha Ramanathan, Biometric Technologies and the Indian Legal System, 54 Econ. & Pol. Wkly. 23 (2019).

GOVERNMENT REPORTS & OFFICIAL PUBLICATIONS :

1. Ministry of Home Affairs, Government of India, Crime in India 2023 Statistics (2023).
2. National Crime Records Bureau, Prison Statistics India 2023 (2023).
3. Unique Identification Authority of India (UIDAI), Aadhaar Authentication Framework (2023).

4. Law Commission of India, Report No. 271: Human DNA Profiling—A Draft Bill for the Use and Regulation of DNA-Based Technology (2017).
5. Parliamentary Standing Committee on Home Affairs, Report on the Criminal Procedure (Identification) Bill, 2022 (2022).

ONLINE SOURCES :

1. AZB & Partners – Biometric Data Regulation in India: Legal Landscape and Risks
2. DW News – India's New Biometric Law Raises Privacy Concerns
3. National Crime Records Bureau
4. Unique Identification Authority of India (UIDAI)
5. European Union GDPR Portal
6. Supreme Court of India Official Website