
RIGHT TO PRIVACY IN THE AGE OF BIOMETRIC TECHNOLOGIES IN INDIA

Evania Irene, Tamil Nadu Dr. Ambedkar Law University, Chennai

ABSTRACT

The increasing use of biometric technologies in India, including facial recognition systems, fingerprint authentication and Aadhar based identification, has significantly altered the relationship between the State and individual privacy. While these technologies promise efficiency, security, and improved governance, they also create serious concerns regarding surveillance, data protection and potential misuse of personal information. This paper examines the constitutional status of the right to privacy under Article 21¹ and evaluates how large scale biometric data collection interacts with established legal principles such as legality, necessity and proportionality. It analyses key judicial developments and the evolving regulatory framework, including recent data protection legislation, to assess whether adequate safeguards exist against arbitrary state action. The study argues that, in the absence of robust oversight mechanisms and clear limitations, biometric surveillance poses a risk to fundamental freedoms. It concludes by emphasising the need for a balanced legal framework that protects individual autonomy while accommodating technological progress.

Keywords: Biometric Technologies, Surveillance, Data Protection, Facial Recognition, Privacy Issues.

¹ INDIA CONST. art. 21.

1. Introduction

Biometric technologies refer to systems that identify or verify an individual based on unique physical or behavioural characteristics. Unlike traditional identification methods such as passwords, identity cards or signatures, biometric systems rely on traits that are intrinsic to a person such as fingerprints, iris patterns, facial features, voice patterns, or even DNA. These technologies have gained significant importance in recent decades due to rapid advancements in digital infrastructure, artificial intelligence, and data processing capabilities.

Initially, biometric tools were largely used for security and law enforcement purposes, particularly in criminal investigations, border control, and access management. However, their use has expanded far beyond these limited functions. In contemporary governance, biometrics are increasingly integrated into welfare delivery, financial services, healthcare systems, digital payments, and public administration. In India, the adoption of biometric technology has been particularly significant due to the scale at which such systems have been deployed. The Aadhar project,² administered by the Unique Identification Authority of India, represents one of the largest biometric identification systems in the world, linking residents' identities through fingerprints and iris scans.

The growth of biometric technologies in India has been accompanied by a significant expansion of surveillance practices. With increasing digitisation, surveillance has moved beyond traditional methods to include biometric authentication, facial recognition, CCTV monitoring, predictive policing, and large-scale personal data collection. These developments have been driven by concerns of national security, crime prevention, and the push toward digital governance. Initiatives such as centralised identity databases, smart city projects, and the use of facial recognition in public spaces reflect a growing reliance on technology-based monitoring.

While such measures are often justified as necessary for security and administrative efficiency, they also raise concerns regarding privacy, legality, and misuse. The possibility of mass surveillance without adequate safeguards creates risks of arbitrary state intrusion and abuse of power. These concerns gained constitutional significance in *Justice K.S. Puttaswamy v. Union*

² Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, No. 18, Acts of Parliament, 2016 (India).

of India,³ where privacy was recognised as a fundamental right and state actions affecting privacy were made subject to legality, necessity, and proportionality.

This research examines the relationship between the right to privacy and the increasing use of biometric technologies in India. It focuses on how biometric systems such as fingerprint recognition, iris authentication, and facial recognition affect privacy rights and whether existing legal safeguards are adequate to address these concerns.

The study aims to analyse the constitutional and regulatory framework governing biometric data, identify risks arising from surveillance practices, and evaluate whether a balance exists between technological advancement, national security, and fundamental rights. It further seeks to identify regulatory gaps and propose reforms to strengthen privacy protection in the digital age.

2. Understanding the Right to Privacy in India

2.1 Evolution of Privacy Jurisprudence

The right to privacy in India has evolved through judicial interpretation rather than explicit constitutional recognition in the original text of the Constitution. In the initial years, privacy was not acknowledged as a separate fundamental right. In *M.P. Sharma v. Satish Chandra* (1954)⁴, the Supreme Court dismissed the notion of a constitutional right to privacy regarding search and seizure. Likewise, in *Kharak Singh v. State of Uttar Pradesh* (1962)⁵, although the majority opinion did not specifically acknowledge privacy as a fundamental right, the ruling paved the way for future recognition by raising concerns related to personal liberty.

Following decisions progressively broadened the scope of privacy protection. In the case of *Gobind v. State of Madhya Pradesh* (1975),⁶ the Court acknowledged that privacy could be inferred from fundamental rights, subject to certain limitations. Subsequent rulings, including *R. Rajagopal v. State of Tamil Nadu* (1994)⁷ and *People's Union for Civil Liberties v. Union of India* (1997)⁸, further enhanced privacy protections, particularly concerning personal

³ Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

⁴ *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300.

⁵ *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.

⁶ *Gobind v. State of Madhya Pradesh*, (1975) 2 SCC 148.

⁷ *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632.

⁸ *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301.

autonomy and the privacy of communications. Through these judgments, privacy jurisprudence expanded gradually until it achieved clear constitutional recognition in 2017.

2.2 Constitutional Basis

The constitutional foundation of the right to privacy lies in Article 21 of the Indian Constitution, which guarantees that no person shall be deprived of life or personal liberty except according to procedure established by law. Through judicial interpretation, Article 21 has been given an expansive meaning, extending beyond mere physical existence to include dignity, autonomy, and individual liberty. Privacy has come to be understood as an essential part of these protections.

The recognition of privacy within Article 21 embodies the notion that individual choices, bodily autonomy, control over information, and protection against unwarranted state interference are essential for living with dignity. Consequently, privacy encompasses more than just physical space; it includes privacy in decision-making, control over personal information, and safeguards against surveillance. This constitutional interpretation has gained particular importance in tackling contemporary issues related to digital technologies and the collection of biometric data.

A major turning point in Indian privacy jurisprudence came with Justice K.S. Puttaswamy v. Union of India, where a nine-judge bench of the Supreme Court unanimously held that the right to privacy is a fundamental right protected under Part III of the Constitution, particularly under Article 21. The Court recognised privacy as intrinsic to life, liberty, dignity, and individual autonomy.

The judgment is significant not only for recognising privacy as a fundamental right but also for laying down principles to assess state interference with privacy. The Court held that any restriction on privacy must satisfy the tests of legality, necessity, and proportionality. These principles have become crucial in evaluating laws and policies involving surveillance, data collection, and biometric technologies. The decision also recognised informational privacy as a key component of privacy rights, making the judgment especially relevant in the context of digital governance and biometric regulation in India.⁹

⁹ Central Information Commission, <https://cic.gov.in/sites/default/files/2012/R2Privacy-Venkatesh.pdf>, (last visited May. 15, 2026)

3. Biometric Technologies in India

Biometric technologies are increasingly used for identification, security and governance. While they improve efficiency and public services, they also raise concerns about privacy and surveillance.

3.1 Facial Recognition Systems

Facial Recognition Technology (FRT) recognises people by examining their facial characteristics. In India, it is employed in law enforcement, airports, and monitoring systems. The proposed Automated Facial Recognition System by the National Crime Records Bureau has sparked worries regarding mass surveillance, insufficient regulation, and potential infringements on privacy as highlighted in Justice K. S. Puttaswamy v. Union of India.

3.2 Aadhar and Fingerprint Authentication

The Aadhaar system, managed by the Unique Identification Authority of India, utilises fingerprints and iris scans for identifying individuals. It has enhanced the delivery of welfare benefits and minimised fraud, yet concerns persist regarding data security, the risk of exclusion from services due to authentication errors, and potential privacy threats.¹⁰ These matters were considered in the case of K. S. Puttaswamy (Aadhaar) v. Union of India.

3.3 Emerging AI based surveillance

The integration of Artificial Intelligence (AI) with biometric surveillance has greatly broadened the possibilities for monitoring in India. AI-driven surveillance merges facial recognition, machine learning, and data analytics to facilitate real-time identification, behaviour tracking, and predictive policing. These technologies are increasingly utilised in smart city initiatives, CCTV networks, and law enforcement frameworks. Unlike conventional surveillance, AI-based systems are capable of not only recording but also analysing patterns, monitoring movements, and automatically identifying individuals. This prompts concerns regarding mass surveillance, profiling, and the potential misuse of personal data. It may also give rise to

¹⁰ Akshansh Pandey, *The Biometric Economy: How India's Biometric Payment System Challenges the Right to Privacy*, WASHINGTON INTERNATIONAL LAW JOURNAL, (December 5, 2025), <https://wilj.org/2025/12/05/the-biometriceconomy-how-indias-biometric-payment-system-challenges-the-right-to-privacy/>

algorithmic bias, incorrect identifications, and infringements on civil liberties.

In the absence of specific legal framework regulating AI driven surveillance in India, serious concerns remain regarding transparency, accountability and protection of the right to privacy. Therefore, while AI based surveillance offers security benefits, it also poses significant constitutional and ethical challenges.

4. Privacy concerns and risks

4.1 Mass Surveillance

The extensive adoption of biometric technologies in India has sparked worries about mass surveillance and its effect on privacy rights. Biometric systems gather distinctive identifiers like fingerprints, facial images, and iris scans, allowing authorities to recognise and monitor individuals on a broad scale. Although these technologies are frequently defended on the basis of security and operational efficiency, excessive surveillance can encroach upon personal liberties.

The implementation of linked databases and monitoring technologies enables ongoing surveillance, frequently without individuals' awareness or consent. This can lead to a "chilling effect," causing individuals to change their behaviours out of concern for being watched. The Puttaswamy judgment's acknowledgment of privacy in the constitution mandates that any surveillance utilising biometric technologies must meet the criteria of legality, necessity, and proportionality.

The use of biometric data on a global scale sparks significant ethical debates regarding surveillance and civil liberties. In India, these concerns are compounded by the country's diverse socio-economic landscape, where issues of social inclusion and equity are paramount. Consequently, ensuring the ethical application of biometric technology, preventing discrimination, and guaranteeing equitable access remain critical priorities.¹¹

4.2 Data Breaches and Misuse

Biometric data is uniquely sensitive due to its permanent nature and intrinsic connection to

¹¹ SCOPE, <https://scope.paruluniversity.ac.in/blog-16.html>, (last visited May 1, 2026).

personal identity. Unlike passwords or identification numbers, biometric traits are not easily replaceable if compromised, meaning data breaches can have enduring repercussions.

The growth of biometric databases elevates the risks of unauthorised access, identity theft, and data misuse. Furthermore, there is the issue of "function creep," in which data gathered for a specific purpose is repurposed for unrelated objectives without the user's consent.¹² These practices pose significant challenges to security, accountability, and the protection of individual privacy.

4.3 Consent and Transparency Issues

Consent is a cornerstone of privacy protection yet, achieving meaningful consent within biometric systems remains a significant challenge. Users often share their biometric data without a complete understanding of how it will be gathered, stored, or utilised, frequently reducing consent to a mere formality rather than a truly informed decision.

Transparency is just as critical, as individuals must be aware of who accesses their information and why. The absence of clear disclosure and the limited control over personal data can erode individual autonomy. Consequently, implementing robust transparency standards and mechanisms for informed consent is vital to safeguarding privacy in the era of biometric technology.

5. Constitutional and Legal Challenges

The swift expansion of biometric technologies in India has introduced significant constitutional and legal complexities surrounding privacy, state authority, and data governance. Although biometric systems have enhanced administrative efficiency and identity verification, their proliferation raises critical concerns regarding the protection of fundamental rights and the sufficiency of current legal safeguards.

5.1 Constitutional Validity and the Aadhaar Framework

A significant development in this area occurred with the Supreme Court's ruling in Justice K.S. Puttaswamy (Aadhaar) v. Union of India, which examined the constitutional legitimacy of the

¹² Office of the Victorian Information Commissioner, <https://ovic.vic.gov.au/privacy/resources-for-organisations/biometrics-and-privacy-issues-and-challenges/>, (last visited May 06, 2026)

Aadhaar system. While the Court affirmed the use of Aadhaar for welfare initiatives, it mandated that the harvesting and processing of biometric data must adhere to strict constitutional criteria. The judgment established that any infringement upon privacy must satisfy the essential tests of legality, necessity, and proportionality. Ultimately, the ruling sought to harmonise state objectives with individual privacy rights, while issuing a stern warning against state overreach.

5.2 Data Protection Framework and the Digital Personal Data Protection Act, 2023

The increasing reliance on biometric data has underscored the necessity for a robust data protection framework. To mitigate risks associated with the collection and processing of personal information, India enacted the Digital Personal Data Protection Act, 2023.¹³ This legislation aims to govern the processing of digital personal data and mandate obligations for organisations that manage such information.

Nevertheless, concerns persist regarding the scope of exemptions and the adequacy of safeguards against the misuse of sensitive data. Given the permanent and highly personal nature of biometric information, rigorous implementation and oversight are critical to ensuring comprehensive privacy protection.

Limitations of the Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023, despite being a significant legislative development, has been criticised for several shortcomings. The Act grants broad exemptions to the State on grounds such as national security and public order, which may dilute privacy protections and enable excessive state intervention. It also fails to provide enhanced safeguards for biometric data despite its permanent and highly sensitive nature. Concerns have further been raised regarding the limited independence of oversight mechanisms, which may affect accountability and enforcement. Additionally, the Act does not adequately regulate emerging issues such as facial recognition technologies, algorithmic profiling, and large-scale surveillance systems, thereby leaving important gaps in the protection of privacy rights in the digital age.

¹³ Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

6. Comparative Perspective

A comparative examination of international privacy frameworks provides valuable guidance in understanding how different jurisdictions regulate biometric technologies while balancing security and fundamental rights. The experiences of the European Union and the United States demonstrate contrasting approaches and offer important lessons for India in developing a more effective legal framework.

The European Union adopts a rights-oriented and precautionary approach toward privacy and biometric regulation. Under the General Data Protection Regulation (GDPR), biometric information is treated as a special category of sensitive data requiring stronger safeguards and strict conditions for processing. In addition to GDPR, the European Union has also introduced regulatory measures under its AI framework to address concerns surrounding facial recognition technologies and biometric identification systems. The regulatory focus extends beyond data collection and considers broader concerns such as proportionality, data minimisation, transparency, and protection of fundamental rights. The EU approach recognises that while biometric technologies can improve security and administrative efficiency, unrestricted deployment may create serious risks for privacy, autonomy, and democratic freedoms. The EU model attempts to ensure that technological advancement does not occur at the cost of individual rights and requires heightened scrutiny before intrusive technologies are used.¹⁴

In contrast, the United States follows a fragmented and sector-based model of privacy regulation. Instead of a comprehensive framework governing biometric and personal data, regulation is distributed across different federal and state laws. Surveillance practices in the United States have frequently generated concerns regarding extensive government monitoring and intelligence gathering. The emphasis on national security objectives has often produced debates regarding the extent to which surveillance powers should be permitted in a democratic society. This approach demonstrates how technological systems developed primarily for security purposes may gradually expand into broader forms of monitoring and data collection.

The comparative experience highlights important lessons for India. First, biometric information requires stronger and distinct safeguards because of its permanent and highly sensitive nature. Second, legal frameworks should incorporate principles such as proportionality, necessity, and

¹⁴ Federica Paolucci, *From Global Standards to Local Safeguards: The AI Act, Biometrics, and Fundamental Rights*, SSRN, 1, 4-8, (2024)

data minimisation while regulating surveillance practices. Third, independent oversight and judicial scrutiny are essential to prevent arbitrary use of biometric technologies. The European experience particularly illustrates that regulation should not merely facilitate technological development but should also ensure that privacy and constitutional rights remain central to governance in the digital age.

7. Conclusion and Suggestions

The increasing use of biometric technologies in India has transformed methods of identification, governance, and service delivery. Technologies such as facial recognition systems, fingerprint authentication, and digital identity mechanisms have improved administrative efficiency and strengthened digital infrastructure. However, the growing dependence on biometric systems has also created significant concerns regarding privacy, surveillance, data security, and individual autonomy. Since biometric information is permanent and closely connected to personal identity, misuse or excessive collection may create long-term consequences for fundamental rights.

The recognition of privacy as a fundamental right under the Puttaswamy judgment marked an important constitutional development by establishing that individual dignity and informational autonomy deserve legal protection. However, the rapid growth of biometric technologies has exposed gaps within the existing legal framework, particularly regarding surveillance practices, consent mechanisms, and protection against misuse of sensitive data. Although legislative measures such as the Digital Personal Data Protection Act, 2023 represent progress, several concerns regarding state exemptions, oversight, and regulation of emerging technologies continue to remain unresolved.

To address these challenges, India should adopt stronger safeguards specifically for biometric data and create a more comprehensive legal framework governing its collection and use. Clear limitations on surveillance practices, stronger transparency requirements, and meaningful consent mechanisms should be introduced. Independent oversight institutions and judicial review processes must also be strengthened to ensure accountability and prevent arbitrary use of power. Further, India may draw lessons from international approaches such as the European model, which emphasises proportionality, data minimisation, and protection of fundamental rights.

Therefore, while biometric technologies offer significant benefits, their deployment must remain consistent with constitutional values and democratic principles. The future of digital governance in India should focus not only on technological advancement but also on preserving privacy, individual dignity, and public trust.