Aadhaar-based biometric authentication in India: A critical study of privacy and data security concerns under constitutional law

Khushi Mogha
Law student
FIMT college, Kapeshera

Abstract

The Aadhaar project represents one of the world's largest biometric identity systems, encompassing more than a billion residents in India. Introduced to ensure efficient delivery of welfare benefits and eliminate leakages in public distribution systems, Aadhaar has significantly transformed digital governance. However, the extensive collection, storage, and use of biometric information have generated serious concerns regarding privacy, informational autonomy, surveillance, and data security. The recognition of privacy as a fundamental right by the Supreme Court in Justice K.S. Puttaswamy v. Union of India marked a constitutional milestone and profoundly influenced the legal assessment of Aadhaar. This paper critically examines the constitutional validity of Aadhaar-based biometric authentication with special emphasis on privacy and data protection concerns. It analyses the constitutional framework under Articles 14, 19, and 21, evaluates significant judicial pronouncements, and studies legislative developments including the Aadhaar and Other Laws (Amendment) Act, 2019 and the Digital Personal Data Protection Act, 2023. The paper argues that although Aadhaar has contributed to administrative efficiency and inclusive governance, deficiencies relating to informed consent, proportionality, data minimisation, and institutional accountability continue to challenge its constitutional legitimacy. The study concludes by proposing reforms aimed at balancing technological innovation with the protection of fundamental rights in a constitutional democracy.

Keywords: Aadhaar, Biometric Authentication, Privacy, Data Security, Constitutional Law, Digital Personal Data Protection.

1. Introduction

One of the most significant initiatives in this regard is the Aadhaar programme, introduced in 2009 and subsequently given statutory recognition through the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. Administered by the Unique Identification Authority of India (UIDAI), Aadhaar assigns a unique twelve-digit identification number to residents based on their demographic and biometric information, including fingerprints, iris scans, and facial images. The Aadhaar project represents the world's largest biometric identification system, encompassing more than a billion individuals. The system

was primarily conceived to eliminate duplication and leakages in welfare schemes, improve transparency in governance, and facilitate direct benefit transfers.

The constitutional debate surrounding Aadhaar gained prominence with the recognition of the right to privacy as a fundamental right by the Supreme Court of India in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017). The Court unequivocally held that privacy is an intrinsic component of the right to life and personal liberty guaranteed under Article 21 of the Constitution and is closely linked with the freedoms guaranteed under Articles 14 and 19. Subsequently, in K.S. Puttaswamy (Aadhaar-5J.) v. Union of India (2018), the Supreme Court upheld the constitutional validity of Aadhaar while imposing important limitations on its use, particularly concerning private entities and data retention. The judgment emphasized the principles of legality, necessity, and proportionality as essential constitutional safeguards in assessing the legitimacy of State action involving personal data. Despite judicial intervention and regulatory safeguards, concerns regarding Aadhaar-based biometric authentication continue to persist.

Digital Personal Data Protection Act, 2023, and the Digital Personal Data Protection Rules, 2025, have introduced a comprehensive framework for regulating digital personal data in India. These developments seek to strengthen data governance through principles such as consent, purpose limitation, accountability, and data minimization. Nevertheless, debates continue regarding the adequacy of existing safeguards, the scope of governmental exemptions, and the effectiveness of institutional oversight mechanisms in protecting citizens' privacy rights. Against this backdrop, the present study critically examines the constitutional dimensions of Aadhaar-based biometric authentication in India, with particular emphasis on privacy and data security concerns. The study analyses the evolving jurisprudence of the Supreme Court, legislative and regulatory developments, and the broader implications of Aadhaar on constitutional governance in the digital age. It seeks to evaluate whether the existing legal framework sufficiently balances the legitimate objectives of the State with the fundamental rights of individuals in a democratic constitutional order.

2. Constitutional Framework Governing Aadhaar

2.1 Article 14: Equality before Law: Guarantees equality before the law and prohibits arbitrary State action. Mandatory biometric authentication may lead to exclusion of vulnerable populations due to authentication failures, thereby resulting in discriminatory treatment. Instances of biometric mismatch, connectivity issues, and technological failures disproportionately affect elderly persons, manual labourers, and residents in remote areas.

2.2 Article 19: Freedom and Informational Autonomy: The compulsory disclosure of personal information may restrict individual autonomy and freedom of expression. Excessive data collection may create a chilling effect, discouraging citizens from exercising constitutional freedoms.

2.3 Article 21: Right to Life and Personal Liberty: It has been judicially interpreted to encompass privacy, dignity, and autonomy. Since biometric information is intrinsically linked to bodily integrity, any State intrusion must satisfy constitutional standards of fairness, reasonableness, and proportionality.

3. Sections

3.1 *Sec. 43A of the Information Technology Act, 2000*, and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, impose liability on entities handling sensitive personal data, including biometric information, for failure to implement adequate security measures, resulting in unauthorized access, disclosure, or misuse of such data.

3.2 *Sec. 45 of IEA & Sec. 39 of BSA* - Opinion of experts, which allows the court to rely on the opinion of experts, such as forensic experts or fingerprint examiners, regarding matters within their expertise, including the identification of individuals based on biometric evidence.

3.3 *Sec. 47 of IEA & Sec. 41(1) of BSA* - Opinion as to handwriting when relevant which permits the court to consider opinions regarding handwriting, signatures, and finger impressions given by experts who are skilled in the examination of such evidence.

3.4 *Sec. 73 of IEA & Sec. 72 of BSA*- Comparison of signature, writing, or seal with others admitted or proved which enables the court to compare disputed signatures, writings, or seals with genuine specimens admitted or proved to determine their authenticity and admissibility as evidence.

3.5 *Sec. 45A of IEA & Sec. 39(2) of BSA* - Opinion of examiner of electronic evidence which by an amendment in 2013, introduced this Sec. which allows the court to rely on the opinion of examiners of electronic evidence, which may include biometric data stored in electronic form, in matters related to the authenticity and admissibility of such evidence.

3.6 *Sec. 4 of Cr.P.C. & BNSS* - Trial of offences under the IPC 1860 (BNS 2023) and other laws, which establishes the authority of the Code of Criminal Procedure to govern the trial of offences, including those involving the collection and presentation of biometric evidence in criminal proceedings.

3.7 *Sec. 53 of Cr.P.C. & Sec. 51 of BNSS* - Examination of accused by medical practitioner at the request of police officer, which empowers the police to require an accused person to undergo medical examination, which may include the collection of biometric data such as fingerprints, for the purpose of investigation and identification.

***3.8** Sec. 165 of Cr.P.C. & Sec. 185 of BNSS* - Search by police officer in the absence of warrant, which confers upon police officers the authority to conduct searches, including the seizure of biometric evidence, without a warrant under certain circumstances, such as when there are reasonable grounds to believe that such evidence is necessary for the investigation of an offence.

4. Privacy Concerns in Aadhaar-Based Biometric Authentication

4.1 Collection of Sensitive Biometric Data

Aadhaar requires submission of fingerprints, iris scans, and facial images. Unlike passwords, biometric attributes cannot be altered once compromised. Consequently, unauthorised access may cause irreversible harm.

4.2 Surveillance and Profiling

Centralised storage and extensive authentication records create possibilities of mass surveillance and profiling by State authorities. Critics argue that aggregation of personal information undermines informational privacy and democratic freedoms.

4.3 Function Creep

The gradual expansion of Aadhaar beyond welfare schemes into banking, telecommunications, transportation, and private transactions raises concerns regarding "function creep," whereby data collected for one purpose is utilised for unrelated purposes.

4.4 Exclusion and Authentication Failure

Authentication failures have resulted in denial of essential welfare benefits to genuine beneficiaries. Such exclusion directly implicates the constitutional right to life and dignity under Article 21.

5. Data Security Concerns

Centralised Database Risks the Central Identities Data Repository (CIDR) stores vast quantities of sensitive information. Centralisation creates a single point of vulnerability, increasing the risk of cyberattacks and unauthorised access. Data Breaches and Leakages Several reports have highlighted incidents involving unauthorised disclosure of Aadhaar-related information. Although UIDAI maintains that core biometric information remains secure, concerns regarding demographic data leaks persist. Informed Consent Deficit Meaningful consent requires transparency regarding collection, processing, storage, and sharing practices. In many instances, users lack adequate understanding of how their data is processed. Biometric Permanence Unlike passwords, biometric identifiers are immutable. Once compromised, individuals cannot replace fingerprints or iris patterns, making robust security measures imperative.

6. Aadhaar and the Digital Personal Data Protection Act, 2023

The enactment of the Digital Personal Data Protection Act, 2023 represents a significant milestone in India's privacy jurisprudence. The Act regulates the processing of digital personal data and establishes rights and obligations concerning such processing. Aadhaar Data as Personal Data Biometric information collected under Aadhaar clearly falls within the ambit of "personal data" under the DPDP Act because such information relates to identifiable individuals. Accordingly, UIDAI, Authentication User Agencies, and associated entities processing Aadhaar data may qualify as Data Fiduciaries. Consent and Lawful Processing the DPDP Act recognizes consent as a primary basis for processing personal data. Consent must be free, specific, informed, unconditional, and unambiguous. However, concerns arise regarding the voluntariness of consent in the Aadhaar framework. Individuals seeking welfare benefits may possess limited practical alternatives, thereby raising doubts regarding the genuineness of consent.

7. Rights of Data Principals and Obligations of Data Fiduciaries

7.1 Right to access information: A data principal has the right to obtain information from the data fiduciary regarding the personal data being processed. This includes details about the categories of data collected, the purpose of processing, and the identities of entities with whom the data has been shared.

7.2 Right to correction and erasure: Individuals may request correction, completion, updating, or erasure of their personal data if it is inaccurate, incomplete, or no longer necessary for the purpose for which it was collected. The data fiduciary is required to comply with such requests unless retention is mandated by law.

7.3 Right to grievance redressal: The Act provides individuals with the right to seek redress for grievances related to the processing of their personal data. Data fiduciaries must establish an effective grievance redressal mechanism, and unresolved complaints may be escalated to the appropriate authority.

7.4 Right to nominate another person: A data principal may nominate another individual to exercise their rights under the Act in the event of death or incapacity. This provision ensures continuity in the protection and management of the data principal's personal data.

Implement reasonable security safeguards, protect personal data against unauthorized processing and notify personal data breaches to erase personal data when no longer necessary; and establish grievance redressal mechanisms. These obligations impose significant responsibilities upon entities involved in Aadhaar authentication.

8. Critique of the DPDP Act, 2023 in the Context of Aadhaar

Although the DPDP Act strengthens India's data protection framework, certain limitations remain. First, the Act does not explicitly classify biometric information as sensitive personal data requiring enhanced protection. Given the unique nature of biometric identifiers, a separate category with stricter safeguards may be desirable. Secondly, the Act grants broad exemptions to State instrumentalities on grounds such as national security, sovereignty, and public order. Excessive exemptions may dilute privacy protections and permit disproportionate governmental access to personal data. Thirdly, concerns persist regarding the independence and effectiveness of enforcement mechanisms, particularly the functioning of the Data Protection Board. Finally, the absence of comprehensive transparency obligations may limit accountability within the Aadhaar ecosystem.

9. Judicial Response: Landmark Case Laws

- **Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)**

The nine-judge Bench unanimously recognised privacy as a fundamental right under Articles 14, 19, and 21 of the Constitution. The Court held that any restriction on privacy must satisfy the tests of legality, necessity, proportionality, and procedural safeguards.

- **Justice K.S. Puttaswamy (Aadhaar-5J.) v. Union of India (2018)**

The Supreme Court, by a majority of 4:1, upheld the constitutional validity of Aadhaar while striking down or reading down several provisions. The Court: Upheld Section 7 relating to welfare benefits. Struck down mandatory linking of Aadhaar with bank accounts. Invalidated mandatory linkage with mobile numbers. Read down provisions permitting private entities unrestricted access. Emphasised proportionality and data minimisation principles. Justice D.Y. Chandrachud, in his dissent, held the Aadhaar Act unconstitutional, highlighting concerns regarding surveillance, exclusion, and procedural irregularities.

- **Recent Judicial Developments In Ajay Kumar Jha v. UIDAI (2025),**

the court reiterated statutory limitations on disclosure of Aadhaar-related information and reaffirmed that sharing of authentication records is permissible only in accordance with Section 33 of the Aadhaar Act. Recent petitions before the Supreme Court continue to question the expansion of Aadhaar authentication beyond identity verification and seek stricter limitations on its usage.

10. Legislative Developments and Recent Amendments

- The Aadhaar ecosystem has undergone significant transformations in recent years, particularly with the enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act) and the subsequent notification of the Digital Personal Data Protection Rules, 2025. These developments seek to establish a comprehensive framework for regulating the collection, processing, storage, and dissemination of digital personal data, including biometric information. However, concerns persist regarding broad exemptions granted to governmental agencies, which may dilute constitutional safeguards under Article 21.

- Another significant development is the expansion of Aadhaar authentication beyond traditional welfare schemes. In 2025, the Government expanded the scope of Aadhaar authentication through the Aadhaar Authentication for Good Governance (Social Welfare, Innovation, Knowledge) Rules, 2025, enabling certain non-government and private entities to utilize Aadhaar authentication for public-interest services. The Aadhaar (Authentication and Offline Verification) Amendment Regulations, 2025 and related amendments encourage secure offline verification, limited data sharing, tokenization, and enhanced user control over personal information.
- **Aadhaar and Other Laws (Amendment) Act, 2019**: The Amendment Act introduces voluntary use of Aadhaar for authentication. Offline verification mechanisms. Enhanced penalties for unauthorised disclosure. Regulation of private entities permitted to undertake authentication. However, critics argue that the amendments inadequately address surveillance concerns.
- **Digital Personal Data Protection Act, 2023**: The Digital Personal Data Protection Act, 2023 represents India's comprehensive data protection framework. Consent-based data processing. Obligations upon Data Fiduciaries. Rights of Data Principals. Data breach notification requirements. Establishment of the Data Protection Board. Nevertheless, exemptions granted to State agencies have attracted criticism for potentially diluting privacy protections. The interaction between the DPDP Act and Aadhaar remains an evolving constitutional issue.

11. Recent Regulatory Developments (2025–2026)

Aadhaar authentication regulations have promoted consent-based offline verification and face authentication mechanisms intended to minimise data exposure and enhance privacy safeguards.

12. Case Studies

12.1 Aadhaar Data Leak Incident (2018)

Background

In 2018, media reports alleged that unauthorized individuals could access Aadhaar-related information through certain online portals for a nominal amount. Personal details of Aadhaar holders were reportedly exposed due to inadequate security controls.

Nature of Privacy Concern

- Unauthorized disclosure of personal information.
- Risk of identity theft.
- Weak access control mechanisms.

Constitutional Implications

The incident raised concerns regarding:

- Informational privacy.
- State accountability.

- Data security obligations.

Link with DPDP Act, 2023

Under the DPDP Act:

- Data Fiduciaries must implement reasonable security safeguards.
- Personal data breaches must be reported.
- Failure to protect data may attract financial penalties.

The incident demonstrates the necessity for stronger cybersecurity measures and breach notification mechanisms.

12.2 Case Study: Exclusion from Welfare Due to Biometric Authentication Failure

Background

Various reports across India documented instances where beneficiaries under the Public Distribution System (PDS) were denied food grains because biometric authentication failed.

Reasons for Failure

- Worn fingerprints of manual labourers.
- Poor internet connectivity.
- Device malfunction.
- Technical errors.

Constitutional Concerns

Such exclusions affect:

- Right to life under Article 21.
- Right to food.
- Equality under Article 14.

Judicial Approach

Courts have repeatedly emphasized that no genuine beneficiary should be denied welfare benefits solely because of authentication failure.

Relevance to DPDP Act, 2023

The DPDP framework should be supplemented with:

- Human oversight mechanisms.
- Alternative modes of identification.
- Effective grievance redressal systems.

12.3 Case Study: Facial Recognition and Expanding Biometric Surveillance

Background

Government agencies increasingly deploy facial recognition technologies for policing, security, and public administration.

Privacy Risks

- Mass surveillance.
- Continuous monitoring.
- Profiling of citizens.
- Chilling effect on free speech.

Constitutional Perspective

The use of facial recognition systems must satisfy the proportionality standards established in Puttaswamy.

Relevance under DPDP Act, 2023

Facial recognition involves processing personal data and therefore requires:

- Lawful processing;
- Transparency;
- Security safeguards; and
- Accountability mechanisms.

The expansion of biometric technologies beyond Aadhaar demonstrates the urgent need for comprehensive privacy regulation in India.

13. Case Laws

13.1 Anuradha Bhasin v. Union of India, (2020) 3 SCC 637

Significance:

- Reinforced the doctrine of proportionality.
- Held that restrictions on digital rights must be necessary, proportionate, and subject to judicial review.
- Important for analyzing digital governance and privacy.

13.2 Internet and Mobile Association of India v. Reserve Bank of India, (2020) 10 SCC 274

Significance:

- Strengthened the proportionality principle in reviewing governmental restrictions affecting digital activities.
- Useful for discussing constitutional scrutiny of technological regulation.

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

Significance:

- Recognized privacy protections against unlawful surveillance.
- Established procedural safeguards for interception of communications.

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

Significance:

- Early recognition of privacy as a constitutional value.
- Laid the groundwork for later privacy jurisprudence.

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

Significance:

- Earlier denied constitutional recognition to privacy.
- Overruled by the Puttaswamy judgment.

14. Conclusion

Aadhaar-based biometric authentication reflects India's transition towards digital governance and welfare efficiency. However, constitutional democracy demands that technological innovation be balanced with the preservation of individual liberty and dignity. The recognition of privacy as a fundamental right has transformed the legal landscape governing biometric identification. While legislative reforms have attempted to strengthen data protection, unresolved concerns relating to surveillance, exclusion, and informational autonomy continue to challenge the constitutional legitimacy of Aadhaar.

Nevertheless, the extensive collection and processing of biometric information create substantial privacy and data security challenges. The constitutional recognition of privacy in the Puttaswamy judgments establishes an essential normative framework for evaluating such challenges. The Digital Personal Data Protection Act, 2023 marks an important step towards safeguarding informational privacy.

Reference

- Bhatia, G. (2019). *The Transformative Constitution: A Radical Biography in Nine Acts*. HarperCollins.
- Government of India. (2016). *The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016*. Government of India.
- Government of India. (2019). *The Aadhaar and Other Laws (Amendment) Act, 2019*. Government of India.
- Government of India. (2023). *Digital Personal Data Protection Act, 2023*. Government of India.
- Kumar, A. (2018). Aadhaar and constitutionalism in India. *Indian Law Review, 2*(2), 127–145.
- Puttaswamy v. Union of India, (2017) 10 SCC 1.
- Puttaswamy (Aadhaar-5J.) v. Union of India, (2019) 1 SCC 1.
- Ajay Kumar Jha v. Unique Identification Authority of India, W.P. (2025).
- Unique Identification Authority of India. (2025). *Aadhaar Authentication and Offline Verification Regulations*. UIDAI.
- Internet Freedom Foundation. (2025) *Aadhaar and Privacy in India: Contemporary Challenges*.
- Justice K.S. Puttaswamy (Retd.) v. Union of India judgment summary. Supreme Court Observer. Retrieved from relevant judicial database.
- International Association of Privacy Professionals. (2018). The Indian Supreme Court's Aadhaar judgment: A privacy perspective.