DOI: 10.21088/jcfs.3107.6874.9226.1

JOURNAL OF CLINICAL FORENSIC SCIENCES
VOLUME 9 NUMBER 2, JULY - DECEMBER 2026

ORIGINAL ARTICLE

Current Legal Perspectives on Biometric Attendance and Data Privacy in India

Samarendra Barman[1], Kaustav Kr Bairagi[2]

HOW TO CITE THIS ARTICLE:

Samarendra Barman, Kaustav Kr Bairagi. Current Legal Perspectives on Biometric Attendance and Data Privacy in India. Jr of Clinical Forensic Sci. 2026; 9(2): 63–66.

ABSTRACT

In recent years, the biometric attendance system has been introduced through executive orders across various sectors, including both governmental and non-governmental organizations, such as medical colleges and hospitals throughout India. This initiative is designed to enhance administrative efficiency, promote punctuality, and track employee productivity. Nevertheless, there are growing worries regarding the dangers of privacy violations, data leaks, and unwarranted monitoring, even with the implementation of a new data protection regime. While the judiciary has not issued a blanket ruling against the mandatory implementation of biometric attendance, it is currently examining petitions and providing insights to encourage the executive branch to refine its execution. Acting as both an employer and a guardian of rights, the judiciary has voiced its concerns and reservations regarding the privacy ramifications and the proportionality of enforcing this system under the current legislative framework.

KEYWORDS

• Biometric attendance system • Data protection regime • Concerns • Judiciary • Privacy • Proportionality

AUTHOR'S AFFILIATION:

[1] Assistant Professor, Department of Forensic Medicine & Toxicology, All India Institute of Medical Sciences, Guwahati, Assam, India.

[2] Additional Professor, Department of Forensic Medicine & Toxicology, All India Institute of Medical Sciences, Guwahati, Assam, India.

CORRESPONDING AUTHOR:

Samarendra Barman, Assistant Professor, Department of Forensic Medicine & Toxicology, All India Institute of Medical Sciences, Guwahati, Assam, India.

E-mail: sam_royale@rediffmail.com

➢ **Received:** 09-05-2026 ➢ **Accepted:** 14-06-2026

Creative Commons Non Commercial CC BY-NC: This article is distributed under the terms of the Creative Commons Attribution NonCommercial 4.0 License (http://www.creativecommons.org/licenses/by-nc/4.0/) *which permits non-Commercial use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the Red Flower Publication and Open Access pages* (https://www.rfppl.co.in)

INTRODUCTION

A biometric attendance system is a time-tracking and access control tool that uses unique biological traits, such as fingerprints, iris scans, etc., to record employee check-ins and check-outs. These systems automate attendance, prevent buddy punching, reduce payroll error, and improve productivity and other human Resource functions. The evolution of India's biometric attendance system began with traditional manual card-based methods, progressing towards the implementation of the Aadhaar Enabled Biometric Attendance System (AEBAS) in 2014 and face-based biometric and geo-fencing attendance in 2025 under the Digital India's initiative to improve transparency and efficiency in public offices.

With widespread implementation of biometric attendance systems, there are growing concerns among the masses about privacy rights, data protection, secondary use, and other ethical and operational challenges associated with such systems. Courts in different jurisdictions have received and heard legal petitions challenging executive notification for mandatory enrolment in biometric attendance systems in various government and non-government offices and establishments. Petitioners argue that mandatory biometric attendance violates the right to privacy established in the K.S. Puttaswamy v. Union of India case. Petitioners contend that biometric data, unlike passwords, cannot be changed, and if compromised, individuals are permanently vulnerable. The Judiciary is concerned about the privacy ramifications and the proportionality of enforcing this system even under the current legislative framework

AEBAS and Digital India Initiatives

AEBAS is an Aadhaar-enabled biometric attendance system that serves as a specific e-governance tool, implemented under the broader Digital India initiative to monitor the attendance of government employees. In November 2014, the Government of India made the Aadhaar Enabled Biometric Attendance System (AEBAS) mandatory for all central government offices in the country. The Department of Personnel and Training (DoPT) issued an Office Memorandum on November 21, 2014, to formalize this decision.[1] The system uses Aadhaar-linked biometric data (fingerprint, iris, or face) for authentication and real-time monitoring. Aadhaar is a twelve-digit unique identity number that can be obtained voluntarily by all citizens of India based on their biometrics and demographic data. The data is collected by the Unique Identification Authority of India (UIDAI), a statutory authority established by the Government of India under the provisions of the Aadhaar Act, 2016.[2]

Statutory regimes for biometric data protection in India

India's legal regime for data protection has transitioned from general e-commerce laws to specialized rules on sensitive personal data, with ongoing legislative efforts to bring a robust and comprehensive data protection law, including biometrics. The early legal framework goes back to the Information Technology (IT) Act, which was introduced in 2000 to govern electronic commerce, digital signatures, and cybercrime. The act did not specifically address privacy or protection of personal data. The act was amended in 2008 to incorporate section 43A which holds a corporate body liable to pay compensation for negligence in implementing "reasonable security practices and procedures" that leads to wrongful loss or gain from a person's sensitive personal data. This section mandates that any establishment or office handling sensitive personal information must adopt adequate security measures to prevent data breaches in any form and shall be held responsible for non-compliance. Nevertheless, the IT Act's primary focus was information security, rather than data protection. While it does regulate certain aspects of personal data use on IT networks within India, it does not provide comprehensive rules or regulations on personal data processing or transfers.[3]

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) SPDI Rules 2011 (Privacy Rules) define personal information and biometrics for the first time in India. The SPDI rules the following set of personal data or information as sensitive viz passwords, financial information, including information relating to bank accounts, credit cards, debit cards, and other payment instrument details, physical, physiological, and mental health condition, sexual orientation, medical records and biometric information.

The Aadhaar Act was introduced in 2016 to provide legal backing to the Aadhaar unique identification number project, which had been in operation before the act came into force. There were numerous litigations filed against the validity of Aadhar biometrics. In September 2018, the Supreme Court of India upheld the constitutional validity of the Aadhaar scheme, stating that the 'Aadhar Act' does not violate an individual's 'Right to Privacy' when he/she agrees to share biometric data.

The Digital Personal Data Protection Act (DPDP Act) was introduced in 2023 and is the only comprehensive data privacy legislation passed till date. The DPDP Act introduces several compliances with respect to the collection, processing, storage and transfer of digital personal data. As of May 2026, the DPDP Act, bolstered by the newly notified DPDP Rules in Nov 2025, has officially entered the implementation phase, creating a new, self-contained regime for digital privacy in India. However, the Act is facing significant constitutional challenges in the Supreme Court, with key concerns focusing on the weakening of transparency laws and increased government surveillance powers. However, the apex court declined to grant an interim stay on the act, meaning implementation continues while the case is heard.

Puttaswamy Standard

The "Puttaswamy Standard" refers to the landmark nine-judge bench judgement of Supreme Court of India in Justice K.S. Puttaswamy vs. Union of India case in 2017, which held that the right to privacy is a fundamental right protected under article 14, 19 & 21 of the Constitution. The judgment established that while privacy is not absolute and can be limited, any restrictions must meet a three-fold test: Legality, Necessity, and Proportionality. This has significant implications for data protection, individual autonomy, and state surveillance in India.[5]

The three-fold Puttaswamy test states that in order for any government legislation to infringe the right to privacy, it must fulfil the following criteria:

Legality, that postulates the existence of a certain law

Necessity, that is defined in terms of a legitimate state objective

Proportionality, which ensures a rational nexus between the objective and the means to achieve the objective. The means to achieve the objective must be the least intrusive means available.

Legal Petitions and Judicial Observation

In recent years, widespread implementation of mandatory biometric attendance through executive notification has raised some serious legal, ethical and human rights concerns. In 2019 the Delhi High Court Issued a notice to the Ministry of AYUSH regarding a petition that challenged the implementation of an Aadhaar-based and geo-location-enabled biometric attendance system in Ayurvedic, Homeopathic, Unani, and Siddha colleges.[6] In September 2024, the Bar Council of India (BCI) mandated the implementation of biometric attendance and CCTV systems in all law colleges across India. The directive was challenged in the Supreme Court by petitioners who argued that the order was unlawful and violated the privacy judgments. In January 2025, the Supreme Court issued a notice to the BCI, directing a response within six weeks.[7] In September 2025, acting on a petition filed by the Haryana Civil Medical Services Association and other petitioners, the Punjab and Haryana High Court has restrained the State of Haryana from taking coercive steps against them over compulsory attendance through the newly introduced Geofencing app.[8] In 2023 Telangana High Court heard multiple petitions concerning biometric attendance, including instances where it was made mandatory in various colleges.[9]

One of the major concerns cited in all those petitions was the lack of any comprehensive data protection legislation. The Digital Personal Data Protection Act, ("DPDPA") which was passed in the parliament in 2023, has not been in force until November 2025. Besides, there are concerns among various employee unions and right advocacy groups that the act would potentially infringe privacy norms set by the Puttaswamy standards because of government exemptions, blanket power on the data protection board, and excessive data collection and surveillance. The act is also criticized for its lack of robust safeguard, diluted consent standards, ambiguous definitions and replacement of the previous compensation model for data breaches.[10]

The Way Forward: Robust data legislation with Constitutional integrity

Biometric data is a unique form of personal, sensitive, and identifiable information. Any breach in the biometric data could lead to irrevocable harm. Friction between the judiciary and the government regarding the personal data regulations mainly focused on fundamental issues, including breaches of constitutional provisions, worries about heightened government surveillance, and amendments to the RTI Act. Given the highly sensitive nature of biometric data, stringent legal and regulatory frameworks must be constructed to govern the collection, storage and management of such data. The government must also consider the concerns raised regarding biometric attendance, taking into account issues of privacy and proportionality.

The DPDP Act, as comprehensive data protection legislation, represents an opportunity to address the unique risks associated with biometric and other sensitive personal information. The act came into force in November 2025 with the government notifying the supporting DPDP Rules, bringing the framework into effect, though full compliance is phased, with major obligations rolling out until mid-2027. However, critics argue that in its current form, the act cannot achieve the confidence of the public due to lack of required specificity and transparency. Several provisions of the act are ambiguous without clear definition, confer broad power to the government for exemptions, undermine the right to information, and contravene the spirit of the fundamental right of privacy guaranteed under the constitution. Despite criticism, the core legal framework of the act is considered final, and as per the government sources, no immediate amendments are currently on the table.[11] However, it is noteworthy that without appropriate changes and amendments in the act, many core ethical and legal issues will remain unresolved. The judiciary and the government should work interdependently to construct a robust legislative framework with constitutional integrity to ensure a secure and trustworthy digital environment for all the citizens.

REFERENCES

1. https://documents.doptcirculars.nic.in/D2/D02est/11013-9-2014-Estt-A-3.pdf
2. https://en.wikipedia.org/wiki/Aadhaar_Act,_2016
3. https://www.khaitanco.com/sites/default/files/2023-12/Data%20Protection%20in%20India %20 Overview%20(w-013-9999) 0.pdf
4. https://law.asia/ai-and-data-protection/
5. "Constitutionality of Aadhaar Act: Judgment Summary". Supreme Court Observer. Retrieved 2 September 2023.
6. https://www.livelaw.in/news-updates/delhi-hc-seeks-ministrys-response-on-plea-against-aadhaar-based-attendance-location-based-recruitment-143483
7. https://www.lawctopus.com/bci-criminal-background-check-biometric-attendance-cctv/
8. https://www.tribuneindia.com/news/haryana/hc-stays-coercive-steps-against-docs-over-attendance-on-geofencing-app/
9. https://www.thehindu.com/news/national/telangana/private-colleges-oppose-sus-biometric-attendance-system/article29369725.ece
10. https://www.medianama.com/2023/08/223-major-concerns-india-data-protection-bill-2023-2/
11. https://economictimes.indiatimes.com/tech/technology/govt-to-make-no-changes-in-dpdp-act-faqs-to-be-issued-soon-sources/articleshow/123190480.cms?from=mdr