Page 305 - 316 **DOI:** *https://doij.org/10.10000/IJLMH.1110417*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 4

2025

Demystifying Biometrics: A Data to be Protected

HARIOM TIWARI[1] AND DARSH PARIKH[2]

ABSTRACT

In the modern world, biometrics has become an integral part of our daily lives. From unlocking smartphones with a fingerprint or facial recognition to accessing secure facilities and verifying identities in financial transactions, biometric systems have revolutionized how we handle security and convenience. By utilizing unique physical or behavioral characteristics, such as fingerprints, iris patterns or voice recognition, biometrics offers a higher level of security compared to traditional methods like passwords and PINs. This technology enhances user experience, reduces fraud, and is often used to streamline processes across various sectors including banking, healthcare, and government services. With the advent of draft DPDP Rules open to suggestions from the general public by Ministry of Electronics and Information Technology, it is high time that the avenue of biometrics be revolutionized by these laws.

Keywords: *Biometrics, Data, Digital Personal Data Protection Act, Sensitive Information, Authentication, Digital Personal Data Protection Rules*

I. INTRODUCTION

In the modern world, biometrics has become an integral and transformative component of our daily lives. This advanced technology is increasingly embedded in various facets of our routine activities, revolutionizing how we approach security, convenience, and efficiency. For instance, biometric systems such as fingerprint and facial recognition technology are now commonplace in smartphones, offering a seamless way to unlock devices with a simple touch or glance. This move towards biometrics not only enhances user convenience but also significantly heightens security compared to traditional methods like passwords and PINs, which are often vulnerable to theft or guesswork.

Beyond personal devices, biometrics plays a crucial role in accessing secure facilities and services. In many organizations, biometric systems are employed to control entry to sensitive areas, ensuring that only authorized personnel can gain access. This application of biometrics extends to financial transactions as well, where fingerprint or iris scans are increasingly used

[1] Author is an LL.M. Student at University of Mumbai, India.
[2] Author is an Advocate at Bombay High Court, India.

 [ISSN 2581-5369]

to verify identities, thereby reducing the risk of fraud and unauthorized access. The advantages of biometrics are evident across various sectors. In banking, for instance, biometric authentication provides an added layer of security that protects against identity theft and fraud, thereby enhancing the safety of online transactions. In healthcare, biometric systems streamline patient identification processes, ensuring accurate medical records and reducing the risk of misidentification. Government services also benefit from biometric technology, with systems in place to manage identities, track entitlements, and streamline administrative processes.

By utilizing unique physical or behavioral characteristics—such as fingerprints, iris patterns, voice recognition, or even facial features—biometric systems offer a superior level of security. Unlike passwords or PINs, which can be forgotten, stolen, or compromised, biometric traits are inherently linked to an individual and are difficult to replicate. This technology not only enhances user experience but also serves as a deterrent to fraud and identity theft, making it an asset in today's digital and physical environments.

Let us look into the laws which play a major role in regulation of biometrics as a form of data. The 3 major laws which governs the overall fields of biometrics are-

a) Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

b) The Aadhar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

c) Digital Personal Data Protection Act, 2023.

Along with the ones mentioned above, it is important to note that MeiTY (Ministry of Electronics and Information Technology) has introduced the Draft Digital Personal Data Protection Rules, 2025. These rules are open to public opinion till March 05, 2025. A summary of the same has been enshrined below:

II. Information technology (reasonable security practices and procedures and sensitive personal data or information) rules, 2011. (IT rules, 2011)

The rules were shared by Central Government's ministry of Communications and Information Technology on 11th April 2011 and was the first official law established by the central government which governed the protection of sensitive data.

The definition of biometrics is defined under the rules as "*the technologies that measure and*

 [ISSN 2581-5369]

analyze human body characteristics, such as fingerprints, eye retinas and irises, voice patterns, facial patterns, hand measurements and DNA for authentication purposes"[3].

The rules are applicable to body corporates. Body corporates are defined under Information Technology Act as- "*Any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities".* [4]The rule generalized companies and did not separate based on nature of the company.

Some of the salient features of the rules are-

Data classified as Sensitive Personal Data or Information (SPDI) under the rules:

- Types of Information covered: Information has been categorized under SPDI as including personal data such as passwords, financial information (credit/debit card details, bank account numbers), health information, sexual orientation, biometric data, and any information that is specifically protected under the rules. (Rule *2(b) of the IT Rules, 2011*.)
- Consent: Collection and processing of SPDI require explicit consent from the individual concerned.

Obligations of Body Corporate and Data Processors on towards the customers

- Security Practices: Organizations (referred to as "body corporate") handling SPDI are required to implement "reasonable security practices and procedures" to protect data from unauthorized access, destruction, or disclosure. This involves adopting and maintaining appropriate security measures.
- Privacy Policy: Organizations must have a privacy policy in place outlining how SPDI is collected, used, and disclosed along with reasonable security practices which are followed by the corporate. This policy shall be published on the website of body corporate. (Rule *4 (1) of the IT Rules, 2011*).

Implementation of Security Practices

- Security Practices: Corporates handling SPDI are required to implement "reasonable security practices and procedures" to protect data from unauthorized access, destruction, or disclosure. Under "reasonable security practices and procedures", a corporate shall be required to give proof that they implemented such security practices and standards and have a comprehensive documented information security programme

[3] Rule 2(1)(b) of the Information Technology Act (Reasonable Security Practices and Procedures and sensitive personal data or information).
[4] Clause (i) of the explanations to Section 43A of the Information Technology Act.

and information security policies that contain managerial, technical, operational and physical security control measures that reflect with the information assets being protected with the nature of business.

- Reasonable Security Measures: Measures include administrative, physical, and technical safeguards. This involves establishing security policies, access controls, encryption, and regular security audits. (*Rule 8(4) of the IT Rules, 2011*)

Data Subject Rights (Rule 5)

- Access and Correction: Individuals have the right to access their SPDI and request corrections if necessary; (*Rule 5 of the IT Rules, 2011*)
- Grievance Redressal: Organizations must provide a mechanism for addressing grievances related to the handling of SPDI.

Transfer of Data (Rule 7)

- Cross-Border Transfer: When transferring SPDI to another country, organizations must ensure that the recipient provides a level of protection comparable to that required under the Indian rules.

Data Retention and Deletion (Rule 5)

- Retention Policy: SPDI should only be retained as long as necessary for the purposes for which it was collected.
- Deletion: Organizations must ensure that SPDI is securely deleted when it is no longer required.

Compliance and Accountability (Rule 8)

- Audits and Reviews: Regular audits and reviews of security practices must be conducted to ensure compliance with the rules.
- Reporting Breaches: Organizations are required to notify the affected individuals and the relevant authorities in case of a data breach involving SPDI.

Penalties and Consequences

- Non-compliance: Failure to adhere to the rules can result in penalties and legal consequences, including compensation for affected individuals and enforcement actions by regulatory bodies.

Overall, the IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, are designed to ensure that sensitive personal data is protected with

 [ISSN 2581-5369]

adequate security measures and to uphold the privacy rights of individuals. These rules aimed to create a framework for managing and securing personal information in a manner that is consistent with international standards and best practices. This was the first step took by the government towards regulating the biometrics space to ensure no mischief is committed.

III. THE AADHAAR (TARGETED DELIVERY OF FINANCIAL AND OTHER SUBSIDIES, BENEFITS AND SERVICES) ACT, 2016

The object behind the act was to provide a legal framework for the issuance and use of the Aadhaar number, a unique identification number based on biometric and demographic data. The primary aim was to streamline the delivery of subsidies, benefits, and services by using Aadhaar for identification and authentication.

Some of the highlights of the act are given below:-

Definition and Scope: the data called "biometric information" is defined as *photograph, fingerprint, Iris scan, or such other biological attributes of an individual as may be specified by regulations.*[5]

- Section 3 authorizes the collection of biometric data for the purpose of assigning Aadhaar numbers and ensures that biometric information is part of the Aadhaar database.

Enrollment and Authentication

- Section 4 outlines the process for Aadhaar enrollment, which includes the collection of biometric data (fingerprints, iris scans, and facial images) along with demographic information. This data is used to generate a unique Aadhaar number for everyone.
- Section 7 provides that Aadhaar is required for availing certain subsidies, benefits, and services. It also establishes that Aadhaar authentication may be required to access these services, which involves verifying biometric data against the Aadhaar database.

Data Security and Privacy

- Section 8 ensures that no person can be denied benefits solely on the grounds of not possessing an Aadhaar number, but they must comply with the requirements if they are otherwise eligible. This includes biometric verification for those who have Aadhaar.

[5] Section 2(g) of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

 [ISSN 2581-5369]

- Section 12 mandates the protection of Aadhaar data, including biometric information. It imposes strict measures for the secure handling of biometric data and prohibits unauthorized use or disclosure.

Usage and Authentication

- Section 9 details the authentication process using Aadhaar, which involves biometric data verification to confirm the identity of individuals. This process is essential for accessing services and benefits linked to Aadhaar.
- Section 10 addresses scenarios where individuals may refuse biometric authentication, allowing for alternative methods of verification if necessary.

Offenses and Penalties

- Section 23 defines offenses related to the misuse or unauthorized access of Aadhaar data, including biometric information. It stipulates penalties for individuals or entities that violate these provisions, ensuring accountability and protection of biometric data.

The Aadhaar Act, 2016, places significant emphasis on biometric data as a core component of the Aadhaar identification system. It ensures that biometric information is collected, stored, and used securely while also establishing mechanisms for authentication and access to services. The Act's provisions related to biometrics aim to enhance the efficiency of service delivery while safeguarding individuals' privacy and data security.

IV. DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act), marks a significant step in data protection legislation in India, focusing on the handling of digital personal data, including sensitive types such as biometric data. The DPDP Act aims to regulate the processing of digital personal data to protect individuals' privacy, ensure data security, and promote responsible data practices. It establishes a legal framework for how personal data, including biometric data, should be collected, used, and safeguarded.

Definition and Scope

- "Personal data"[6] has been defined under the act as any data about an individual who is identifiable by or in relation to such data. (*Biometric data is included under this definition as a type of sensitive personal data due to its unique and personal nature*).

[6] Section 2(t) of the Digital Personal Data Protection

- Section 2(n) defines "digital personal data" as personal data in digital form.

Processing and Consent

- Section 6 requires that personal data, including biometric data, must be processed only with the explicit consent of the data subject. This consent must be informed, specific, and obtained for legitimate purposes.
- Section 4 stipulates that the processing of sensitive personal data, including biometrics, is subject to additional conditions, including obtaining explicit consent and ensuring that data processing is necessary and proportionate.

Data Protection and Security Measures: Section 8(4) mandates that organizations implement reasonable security practices and procedures to protect personal data, including biometric information, from unauthorized access, loss, or breaches.

Rights of Data Subjects: Section 14 grants data subjects the right to access their personal data, including biometric data, and provides individuals with the right to withdraw consent for the processing of their personal data, including biometrics, at any time, with the effect that further processing must cease unless otherwise permitted by law.

Data Breach Notification: Section 8 (6) requires organizations to notify the data protection authority and affected individuals in the event of a data breach involving biometric data or other personal data. This notification must be timely and include details of the breach and measures taken to address it.

Compliance and Enforcement: Section 18 establishes the role of the Data Protection Authority of India (DPA) in overseeing compliance with the DPDP Act, including monitoring the handling of biometric data and enforcing data protection standards.

Penalties and Liabilities: Section 33 exacts penalties for non-compliance with the Act's provisions, including those related to the mishandling or unauthorized use of biometric data. Organizations found in violation may face significant fines and corrective measures.

The DPDP Act, 2023, represents a comprehensive approach to data protection in India, placing a strong emphasis on the security and ethical handling of personal data, including biometrics. It aims to balance the benefits of data use with the need to protect individual's privacy and ensure responsible data practices.

 [ISSN 2581-5369]

V. DRAFT DIGITAL PERSONAL DATA PROTECTION RULES, 2025

The draft Digital Personal Data Protection (DPDP) Rules, 2025, aimed to operationalize the DPDP Act, 2023, with an intrinsic focus to safeguard the citizens' data privacy rights and establishing a balanced framework for data governance in India. Some of the salient features of the Rules are as follows.

Core Objectives and Approach:

- Citizen-Centric: The rules placed Data Principals at the core, empowering them with greater control over their personal data.
- Digital-First Philosophy: Mechanisms for consent, grievance redressal, and the functioning of the Data Protection Board are designed to be digital, ensuring ease of living and ease of doing business. The Board will operate as a digital office for quick and transparent complaint resolution.
- Balance between Innovation and Regulation: India's framework seeks to balance fostering economic growth with prioritizing citizen welfare, aiming to be a global template for data governance.
- Inclusive Law-Making: The draft rules are based on wide-ranging inputs from stakeholders and global best practices, with public feedback invited.

Key Provisions and Responsibilities:

- Informed Consent: Data Fiduciaries must provide clear and accessible information on data processing, enabling informed consent. Citizens have rights to give, deny, or withdraw consent, and to access records of their consents, notices, and data sharing activities.
- Data Principal Rights: Citizens are empowered with rights to demand data erasure and access user-friendly mechanisms to manage their data.
- Obligations for Data Fiduciaries:
    - Implement reasonable security safeguards to prevent personal data breaches.
    - Maintain records of consents, notices, and data sharing for at least 7 years.
    - Provide a website or app as the primary means for Data Principals to manage consent and access services.
    - Cannot sub-contract or assign obligations under the Act and rules.

- For e-commerce platforms, online gaming intermediaries, and social media platforms, data retention policies mandate deletion of user data after three years unless the user actively maintains their account.
- Significant Data Fiduciaries have higher obligations, including provisions for annual data protection impact assessments and audits to ensure compliance.

- Children's Data: Data Fiduciaries must implement appropriate technical and organizational measures to obtain verifiable consent from a child's parent or legal guardian. Processing children's personal data is restricted to specific activities like health services, educational activities, safety monitoring, and transportation tracking, necessary for the child's well-being.
- Consent Managers: Must be companies incorporated in India with sound financial and operational capacity (minimum net worth of Rs. 2 crore), reputation for fairness, and a certified interoperable platform. They must maintain independence to prevent conflicts of interest.

Enforcement and Compliance:

- Data Protection Board: Envisaged as a digital office for quick and transparent resolution of complaints. The Board will consider factors like the nature and gravity of default and efforts made to mitigate impact when imposing penalties.
- Penal Provisions:
  - Failure by a Data Fiduciary to implement reasonable security safeguards: Up to Rs. 250 crores.
  - Failure to notify the Board or affected Data Principal of a personal data breach: Up to Rs. 200 crores.
- Voluntary Undertakings: Data Fiduciaries may voluntarily give undertakings at any stage of proceedings, which if accepted by the Board, can lead to the dropping of proceedings.
- Cross-Border Data Transfers: The rules are expected to clarify regulations regarding international data transfers.
- Exemptions: The draft Rules provide an exemption for personal data processing for research, archiving, or statistical purposes, subject to safeguards.

 [ISSN 2581-5369]

Implementation and Transition:

- A 45-day consultation period was provided for public feedback on the draft rules (deadline February 18, 2025).
- The compliance or transition period under the final rules is likely to be between six to eight months.
- Early-stage startups may receive a grace period (3-6 months) exempting them from certain stringent provisions.
- The government plans a comprehensive awareness campaign to educate citizens about their rights and responsibilities.

These rules signify a major step in India's data privacy landscape, emphasizing accountability, transparency, and user rights, and will require businesses to adopt more structured data governance practices.

VI. Conclusion

Biometrics are classified as sensitive information under the law and are integral to various daily activities, such as unlocking mobile devices and marking attendance. To ensure the secure handling of biometric data, the Company & vendor of the following service shall adhere to the following legal standards and regulations:

1. Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. [IT Rules].
2. Digital Personal Data Protection Act, 2023. [DPDP Act].

The following guidelines shall be followed by a vendor for adherence to law under *IT Rules.*

Under Rule 5 (7) of the IT Rules, Company shall ensure that it has received written consent from all employees whose biometric information it shall process. Before receiving consent, Company shall take steps by which the employee shall have knowledge of-:

- Fact that the information is being collected;
- Purpose for which information is being collected;
- Intended recipients of the information;
- Name and address of agency which collects and retains information.

 [ISSN 2581-5369]

- Consent shall be in writing. The person who provides biometric information to be processed shall be permitted by Company to review information submitted by them and in case of any inaccuracies, can make amendments.
- Withdrawal of consent by person providing the information is allowed in writing. However, under the rule, the same shall result in discontinuing the service for that employee for which biometrics information were sought.

Under rule 4 of the IT Rules, Company shall provide a link with the consent mail redirecting the employee to the privacy policy shared by the vendor which shall include how it handles and deals with biometric data. This privacy policy shall include-

- Clear and easily accessible statement for its practices and policies;
- Type of personal data collected;
- Purpose of data collection;
- Disclosures of information to government agencies;
- Reasonable security practices followed by the vendor.

The contact details of GRO (Grievance Redressal Officer) shall be updated on Company website. On receipt of a complaint regarding consent, processing or leakage of biometric data, GRO shall be responsible for redressal of the issue within span of a month.

Vendor shall follow the following security practices to be considered as complying with reasonable security practices and procedures only if-

- The vendor has comprehensive documented information security programme & information security policies that contain managerial, technical, operational and physical security control measures that commensurate with information assets being protected with nature of business.
- Being an ISO/IE/IEC 27001 certified standard (or)

Any industry association or entity formed by such an association whose members are self regulating by following other than ISO/IS/IEC practices. These codes are to be duly approved by central government.

The vendor who is approved under ISO/IE/IEC or code of best practices shall be deemed to follow reasonable security practices if their standard is certified (or) audited on a yearly basis.

The following guidelines shall be followed by the vendor for adherence to law under *DPDP Act.*

 [ISSN 2581-5369]

- For processing personal data, written consent shall be took from all persons who are sharing their biometric information. For requesting consent, a notice (in form of intimation via mail) shall be given to all employees which shall include-
    - Type of personal data and purpose for which biometric data is processed;
    - The process of Withdrawal of consent and filing grievance for processing biometric data;
    - Manner in which complaint can be made to Data Protection Board of India.
- The request for consent shall be shared with the employee in clear and plain language and shall contain information of Data Protection Officer (Chief Information Security Officer) who shall be held answerable on behalf of Company, if any questions are raised by the employee in regards to processing of their personal data.
- In case an employee withdraws their consent (*process for withdrawal of consent not provided in the act*), no biometric data shall be processed and data shall be deleted unless the data is in possession of Company for lawful purposes.
- In the event of biometric data breach, Company shall intimate Data Protection Board and the employee whose data was breached.

*****

 [ISSN 2581-5369]