# INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 6 AND ISSUE 1 OF 2026

INSTITUTE OF LEGAL EDUCATION

# INDIAN JOURNAL OF LEGAL REVIEW

**APIS – 3920 – 0001 | ISSN - 2583-2344**

**(Open Access Journal)**

**Journal's Home Page – https://ijlr.iledu.in/**

**Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/**

**Volume 6 and Issue 1 of 2026 (Access Full Issue on - https://ijlr.iledu.in/volume-6-and-issue-1-of-2026/)**

**Publisher**

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 73059 14348 - info@iledu.in / Chairman@iledu.in


INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 1 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

# THE DIGITAL PERSONA IN PERIL: ANALYZING THE DECRIMINALIZATION PARADOX IN INDIA'S BIOMETRIC DATA LAWS

**AUTHOR -** ARCHI ARYA* & DR.MUDRA SINGH**

* LLM. (CRIMINAL LAW), AMITY LAW SCHOOL, AMITY UNIVERSITY UTTAR PRADESH, LUCKNOW CAMPUS

** ASSISTANT PROFESSOR AR AMITY LAW SCHOOL, AMITY UNIVERSITY UTTAR PRADESH, LUCKNOW CAMPUS

**BEST CITATION** - ARCHI ARYA & DR.MUDRA SINGH, THE DIGITAL PERSONA IN PERIL: ANALYZING THE DECRIMINALIZATION PARADOX IN INDIA'S BIOMETRIC DATA LAWS, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (1) OF 2026, PG. 653-659, APIS – 3920 – 0001 & ISSN - 2583-2344.

**ABSTRACT**

*The integration of biometric authentication into India's governance infrastructure has fundamentally altered the relationship between the citizen and the State, creating a "digital persona" susceptible to surveillance and commercial exploitation. This research paper provides a doctrinal analysis of the evolving legal architecture governing biometric data in the "post-Puttaswamy" era, where the Supreme Court's recognition of the fundamental right to privacy serves as the normative baseline for data protection.*

*The study examines the fragmented statutory landscape, juxtaposing the rigorous criminal penalties of the Aadhaar Act, 2016, and the Information Technology Act, 2000, against the nascent civil liability regime introduced by the Digital Personal Data Protection Act, 2023 (DPDP Act). It traces the jurisprudential shift from the "spatial" privacy of early case law to the "informational privacy" established in Justice K.S. Puttaswamy v. Union of India (2017), which mandated a tripartite test of legality, necessity, and proportionality for state intrusion.*

*Furthermore, the paper evaluates the "decriminalization paradox" emerging from the DPDP Act, which replaces imprisonment with monetary penalties, potentially weakening the deterrence framework for individual data breaches. By mapping these statutes against surveillance risks, the research concludes that while India has transitioned toward a consent-centric regime, significant lacunae remain regarding the regulation of state surveillance and the classification of biometric data thefnder the Bharatiya Nyaya Sanhita, 2023.*

**Keywords:** Biometric Data, Right to Privacy, Puttaswamy, Aadhaar Act, DPDP Act 2023, Data Surveillance.

## 1.0 Introduction

The governance of biometric data constitutes one of the most complex and contentious frontiers in Indian constitutional and statutory law. As the nation transitions to a digitally empowered society, the human body, through fingerprints, iris scans, and facial patterns, has become the primary means of authentication for accessing state welfare, banking services, and telecommunications. This paradigm shift, epitomised by the world's most extensive biometric identity program, Aadhaar, has fundamentally altered the relationship between the citizen and the State, necessitating a rigorous legal framework to protect the "digital persona" from surveillance, theft, and misuse.

This chapter provides an exhaustive analysis of the legal architecture governing biometric data in India. It situates the discussion in the "post-Puttaswamy" era, acknowledging that the

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 1 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

landmark 2017 Supreme Court judgment recognising privacy as a fundamental right has become the normative baseline against which all data practices are measured. The analysis dissects the fragmented statutory landscape, ranging from the specific mandates of the Aadhaar Act, 2016, and the Information Technology Act, 2000, to the nascent but transformative regime introduced by the Digital Personal Data Protection Act, 2023 (DPDP Act). Furthermore, it critically examines the lingering penal provisions of the Indian Penal Code (IPC) and the Bharatiya Nyaya Sanhita (BNS), which struggle to categorise intangible biometric data within traditional definitions of "property" and "theft."

Through a doctrinal mapping of statutes to surveillance risks, this chapter argues that, while India has moved towards a consent-centric data protection regime, significant lacunae remain in criminal enforcement of biometric breaches and in the regulation of state surveillance.

### 3.1 Constitutional Provisions: The Fundamental Right to Privacy

The constitutional protection of biometric data in India is not derived from a single textual provision but is a jurisprudential construct evolved by the Supreme Court of India. This evolution traces a trajectory from an initial denial of privacy as a guaranteed right to its current status as an intrinsic part of the Right to Life and Personal Liberty under Article 21 of the Constitution.

#### 1.1.1 Historical Context: The Pre-Puttaswamy Era

For decades, the Indian legal framework governing privacy has been characterised by ambiguity. Early Supreme Court judgments, specifically *M.P. Sharma v. Satish Chandra*[1535] and *Kharak Singh v. State of Uttar Pradesh*[1536], were interpreted by the State to mean that the Constitution did not guarantee a fundamental right to privacy. In *M.P. Sharma*, an eight-judge bench held that the drafters of the Constitution did not intend to subject the power of search and seizure to a fundamental right of privacy. Similarly, *Kharak Singh*, while striking down police domiciliary visits, held that the right to privacy was not guaranteed under the Constitution.

#### 1.1.2 Justice K.S. Puttaswamy v. Union of India (2017): The Privacy Judgment

On August 24, 2017, a nine-judge Constitution Bench of the Supreme Court delivered a unanimous verdict in *Justice K.S. Puttaswamy (Retd.) v. Union of India.*[1537], overruling *M.P. Sharma* and *Kharak Singh*. The Court held that the Right to Privacy is a fundamental right protected under Article 21 and is intrinsic to human dignity and liberty.

**Informational Privacy and Biometrics:**

The judgment went beyond a spatial understanding of privacy (the privacy of the home) to explicitly recognise "informational privacy." Justice D.Y. Chandrachud (as he then was), writing for the plurality, noted that privacy includes the right to control the dissemination of personal information. The Court recognised that biometric data constitutes a powerful tool for profiling. Aggregated data combining biometrics with demographic and transactional records can reveal intimate details about an individual's political beliefs, health, sexual orientation, and financial status, thereby creating a "surveillance state" if left unchecked.

**The Three-Pronged Test (Proportionality):**

To balance the State's legitimate interests with the individual's right to biometric privacy, the Court established the "Proportionality Test." Any state invasion of privacy must satisfy three requirements:

1. **Legality:** The existence of a valid law.
2. **Necessity:** The law must have a legitimate State aim.

[1535] *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300.
[1536] *Kharak Singh v. State of U.P.*, AIR 1963 SC 1295.
[1537] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 1 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

3. **Proportionality:** There must be a rational nexus between the object and the means adopted, and the intrusion must be the least restrictive method available.[1538]

### 1.1.3 Puttaswamy II (2018): The Validity of the Aadhaar Act

Following the declaration of privacy as a fundamental right, a five-judge bench examined the specific constitutionality of the Aadhaar Act, 2016, in *Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors.* (2018)[1539]. The petitioners argued that the centralised storage of biometric data in the Central Identities Data Repository (CIDR) created a permanent risk of mass surveillance.

The Supreme Court upheld the constitutionality of the Aadhaar Act but significantly "read down" several provisions to align them with the proportionality test:

- **Strike Down of Section 57:** The Court struck down Section 57, which had permitted private entities (banks, telecom operators) to use Aadhaar biometrics for authentication pursuant to a contract, holding it disproportionate.
- **Data Minimisation:** The Court upheld the collection of biometric data for welfare schemes, accepting the government's argument that it was necessary to prevent "ghost beneficiaries" under Section 7 of the Act.
- **Data Retention:** The Court struck down regulations allowing the archiving of authentication transaction logs for five years, reducing the retention period to six months.

### 1.1.4 Article 20(3) and Bodily Integrity

The protection of biometric data is also linked to Article 20(3) of the Constitution, which protects against self-incrimination. In *Selvi v. State of Karnataka*[1540], the Supreme Court held that involuntary administration of neuro-scientific tests violates Article 20(3) and Article 21. While *Puttaswamy II* distinguished Aadhaar enrolment from the *Selvi* context, the principle remains that the state cannot compel the surrender of biometric data for criminal investigation without a specific statutory framework adhering to due process, a concern relevant to the *Criminal Procedure (Identification) Act, 2022*.

## 1.2 Key Statutes: Mapping the Regulatory Framework

In the absence of a single, unified data protection code for many years, India's regulation of biometric data has been governed by a patchwork of sector-specific laws.

### 1.2.1 The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

The Aadhaar Act is the primary legislation governing biometric data in India and establishes the Unique Identification Authority of India (UIDAI).

**Provisions on Biometric Protection:**

- **Section 29 (Restriction on Sharing):** Section 29(1) prohibits the sharing, disclosing, or displaying of "core biometric information" (fingerprints and iris scans). Section 29(2) restricts the use of identity information only for the purpose specified at authentication.[1541]
- **Section 28 (Security and Confidentiality):** Imposes a statutory duty on the UIDAI to ensure the security of identity information and mandates confidentiality.[1542]
- **Section 30:** Deems biometric information to be "electronic record" and "sensitive personal data or information" (SPDI),

[1538] *Id.* at para 310.
[1539] *Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors.*, (2019) 1 SCC 1.
[1540] *Selvi v. State of Karnataka*, (2010) 7 SCC 263.
[1541] The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, s. 29.
[1542] *Id.*, s. 28.

attracting protections under the IT Act, 2000.[1543]

**Criminal Penalties for Biometric Misuse:**

- **Unauthorised Access to CIDR (Section 38):** Punishes intentional access, downloading of data, or disruption of the CIDR with imprisonment extending to 10 years and a fine not less than ₹10 lakh.[1544]
- **Tampering with Data (Section 39):** Tampering with data in the CIDR is punishable by imprisonment up to 10 years.[1545]
- **Impersonation (Section 34):** Providing false biometric information to impersonate an Aadhaar holder is punishable by imprisonment up to 3 years.[1546]

### 1.2.2 The Information Technology Act, 2000 (as amended)

Until the full operationalisation of the DPDP Act, the IT Act remains the general statute governing the protection of biometric data in the private sector.

**Section 43A and SPDI Rules:**

Section 43A requires body corporates handling "sensitive personal data or information" (SPDI) to maintain reasonable security practices. Negligence resulting in wrongful loss renders the entity liable to pay damages.[1547]

- **Rule 3 of SPDI Rules, 2011:** Explicitly defines "Biometric information" as Sensitive Personal Data.[1548]

**Criminal Provisions under the IT Act:**

- **Section 66 (Computer Related Offences):** Criminalises dishonest or fraudulent acts referred to in Section 43 (e.g., unauthorised access), punishable with imprisonment up to 3 years.[1549]
- **Section 66C (Identity Theft):** Punishes the fraudulent use of another person's "unique identification feature" (including biometrics) with imprisonment up to 3 years.[1550]
- **Section 72A:** Punishes disclosure of personal information obtained under a lawful contract without consent, with imprisonment up to 3 years.[1551]

### 1.2.3 Indian Penal Code (IPC), 1860 and Bharatiya Nyaya Sanhita (BNS), 2023

The application of criminal law to biometric data theft involves interpreting "data" as property.

**The "Data as Property" Debate:**

- **Theft (Section 378 IPC):** Theft requires the subject to be "movable property." In *R.K. Dalmia v. Delhi Administration*[1552]The Supreme Court held that "property" is used in a broad sense. In *Pyare Lal Bhargava v. State of Rajasthan*[1553]The Court held that even the temporary removal of a file to copy it constitutes theft. This logic extends to copying biometric databases.
- **Electricity as Property:** In *Jagjit Singh v. State of Punjab*[1554]The court recognised intangible energy as subject to theft, thereby supporting the classification of digital data as movable property.

**Transition to Bharatiya Nyaya Sanhita (BNS), 2023:**

- **Section 303 (Theft):** The BNS modernises the definition to cover digital assets as movable property explicitly, punishing theft with imprisonment up to 3 years.[1555]

[1543] *Id.*, s. 30.
[1544] *Id.*, s. 38.
[1545] *Id.*, s. 39
[1546] *Id.*, s. 34.
[1547] The Information Technology Act, 2000, s. 43A.
[1548] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, r. 3.
[1549] The Information Technology Act, 2000, s. 66.
[1550] *Id.*, s. 66C.
[1551] *Id.*, s. 72A.
[1552] *R.K. Dalmia v. Delhi Administration*, AIR 1962 SC 1821.
[1553] *Pyare Lal Bhargava v. State of Rajasthan*, AIR 1963 SC 1094.
[1554] *Jagjit Singh v. State of Punjab*, 1996 Cr LJ 2962.
[1555] The Bharatiya Nyaya Sanhita, 2023, s. 303.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 1 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

- **Section 318 (Cheating):** Replaces IPC Section 420, covering deception involving biometric fraud.[1556]

### 1.3 Emerging Laws: The Digital Personal Data Protection Act, 2023

The **Digital Personal Data Protection Act, 2023 (DPDP Act),** introduces a high-penalty, civil liability regime.

#### 1.3.1 Definition and Scope

The Act governs "digital personal data." Unlike the SPDI Rules, it does not categorise "biometrics" separately; instead, it applies a single standard of protection. Entities handling large biometric databases may be classified as "Significant Data Fiduciaries" (SDFs).[1557]

#### 1.3.2 Consent and Legitimate Uses

- **Section 6:** Mandates "free, specific, informed, unconditional, and unambiguous" consent.[1558]
- **Section 7 (Legitimate Uses):** Allows processing without consent for specified purposes, such as state welfare benefits, providing a legal basis for government biometric authentication.[1559]

#### 1.3.3 Decriminalisation and Civil Penalties

The DPDP Act decriminalises data protection offences, replacing imprisonment with monetary penalties imposed by the Data Protection Board.

- **Section 33 & Schedule:** Imposes penalties up to **₹250 crore** for failure to take reasonable security safeguards to prevent a personal data breach.[1560]

### 1.4 Regulatory Bodies

- **UIDAI:** Est. under Aadhaar Act; regulates the Aadhaar ecosystem and imposes civil penalties.[1561]
- **CERT-In:** Under *CERT-In Directions, 2022*, mandates reporting of cyber incidents (including biometric breaches) within **6 hours**.[1562]
- **Data Protection Board of India:** Est. under DPDP Act; adjudicates non-compliance and imposes penalties.[1563]

### 1.5 Gaps in the Framework

- **Decriminalization Paradox:** While the Aadhaar Act retains 10-year imprisonment for CIDR breaches, the DPDP Act removes criminal liability for general biometric breaches, relying only on fines. This creates a deterrence gap for individual hackers.[1564]
- **Surveillance Risks:** Section 17 of the DPDP Act allows broad exemptions for government instrumentalities, potentially permitting unrestricted biometric surveillance (e.g., Facial Recognition Technology) without the oversight mandated by *Puttaswamy*.[1565]

### Conclusion

The governance of biometric data in India has traversed a complex trajectory, evolving from a fragmented sector-specific approach to a constitutionally entrenched fundamental right. As this research demonstrates, the integration of biometric authentication into the delivery of essential state services has fundamentally redefined the social contract, creating a "digital persona" that is vulnerable to both surveillance and commercial exploitation.

The turning point in this legal architecture remains the Supreme Court's landmark verdict in *Justice K.S. Puttaswamy v. Union of India* (2017). By overruling the pre-constitutional stance of *M.P. Sharma* and *Kharak Singh*, the Court firmly established informational privacy as a facet of Article 21, thereby subjecting all

[1556] *d.*, s. 318.
[1557] The Digital Personal Data Protection Act, 2023, s. 10.
[1558] *Id.*, s. 6.
[1559] *Id.*, s. 7.
[1560] *Id.*, Schedule read with s. 33.
[1561] The Aadhaar Act, 2016, s. 23A.
[1562] CERT-In, *Directions under sub-section (6) of section 70B of the Information Technology Act, 2000*, No. 20(3)/2022-CERT-In (April 28, 2022).
[1563] The Digital Personal Data Protection Act, 2023, s. 18.
[1564] *See* Amber Sinha, "The Data Protection Bill's criminal liability problem", *Medianama* (Dec. 2022).
[1565] The Digital Personal Data Protection Act, 2023, s. 17.

state intrusions to the rigorous test of legality, necessity, and proportionality. This jurisprudential baseline was instrumental in the judicial "reading down" of the Aadhaar Act in *Puttaswamy II* (2018), which curbed the unbridled retention of data and prohibited private sector exploitation of the biometric ecosystem.

However, the statutory landscape remains a patchwork of overlapping regimes. While the Aadhaar Act, 2016, imposes stringent criminal penalties for breaches of the Central Identities Data Repository (CIDR), and the Bharatiya Nyaya Sanhita (BNS), 2023, attempts to modernize the definition of theft to include digital assets, significant inconsistencies persist.

The enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act), marks a paradigm shift toward a high-penalty civil liability regime. While it emphasizes "consent-centric" processing and imposes substantial fines for non-compliance, this research identifies a critical "decriminalization paradox." By replacing imprisonment with monetary penalties for general data breaches, the DPDP Act may weaken the deterrence framework for individual offenders compared to the stricter criminal provisions under the Aadhaar Act and the IT Act.

Furthermore, the broad exemptions granted to government instrumentalities under Section 17 of the DPDP Act threaten to undermine the protections guaranteed by *Puttaswamy*. These exemptions create potential avenues for unrestricted biometric surveillance without adequate independent oversight. Consequently, while India has successfully established a legal framework that recognizes the sanctity of biometric data, the current regime leaves "lacunae" regarding criminal enforcement and checks on state power. Future legal reforms must address these gaps to ensure that the transition to a digitally empowered society does not come at the cost of the citizen's constitutional right to privacy and bodily integrity.

**BIBLIOGRAPHY**

**A. Primary Sources: Statutes and Regulations**

1. **The Constitution of India, 1950**
   - *Relevant Articles cited*: Article 21 (Right to Life and Personal Liberty), Article 20(3) (Protection against Self-Incrimination).
2. **The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016**
   - *Relevant Sections cited*: Sections 7, 28, 29, 30, 33, 34, 38, 39, and 57.
3. **The Bharatiya Nyaya Sanhita (BNS), 2023**
   - *Relevant Sections cited*: Section 303 (Theft), Section 318 (Cheating).
4. **The Criminal Procedure (Identification) Act, 2022**.
5. **The Digital Personal Data Protection Act (DPDP Act), 2023**
   - *Relevant Sections cited*: Sections 6, 7, 17, 33, and Schedule.
6. **The Indian Penal Code (IPC), 1860**
   - *Relevant Sections cited*: Section 378 (Theft), Section 420 (Cheating).
7. **The Information Technology Act, 2000 (as amended)**
   - *Relevant Sections cited*: Sections 43A, 66, 66C, 72A.
8. **Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011**
   - *Relevant Rules cited*: Rule 3.
9. **CERT-In Directions, 2022**
   - *Relevant Mandates cited*: Cyber incident reporting timeline (6 hours).

**B. Primary Sources: Case Law (Supreme Court of India)**

1. *Jagjit Singh v. State of Punjab*.
2. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) (The Privacy Judgment).
3. *Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors.*, (2018) (The Aadhaar Judgment).
4. *Kharak Singh v. State of Uttar Pradesh*, (1963).
5. *M.P. Sharma v. Satish Chandra*, (1954).
6. *Pyare Lal Bhargava v. State of Rajasthan*.
7. *R.K. Dalmia v. Delhi Administration*.
8. *Selvi v. State of Karnataka*, (2010).