

Biometric Databases, Facial Recognition, And the Constitutional Value of Bodily Integrity: An Indian Perspective

Yougank Khare

Asst. Professor, Jabalpur (M.P.)

Abstract—India's expansion of biometric identification systems—particularly the Aadhaar programme enrolling over 1.3 billion residents and the proliferation of facial recognition technology in law enforcement and welfare delivery—raises profound constitutional questions about the scope and protection of bodily integrity under Article 21 of the Indian Constitution. This paper examines whether the collection, storage, and deployment of biometric markers (fingerprints, iris scans, facial photographs) and their integration into networked databases constitute an unconstitutional encroachment on bodily integrity, a fundamental aspect of the right to privacy. Drawing on the Supreme Court's landmark privacy judgments in *Puttaswamy* (2017) and the Aadhaar case (2018), this paper argues that current legal protections inadequately safeguard bodily integrity against the unique risks posed by biometric surveillance. The paper identifies critical gaps in existing legislation (the Aadhaar Act, 2016 and the Digital Personal Data Protection Act, 2023) and highlights how facial recognition amplifies these risks through covert, mass, and discriminatory tracking. Ultimately, the paper proposes a strengthened constitutional and legislative framework anchoring bodily integrity protection in principles of necessity, consent, data minimization, and independent oversight, essential for reconciling technological governance with democratic dignity.

Index Terms—bodily integrity, biometric data, facial recognition, Article 21, privacy rights, Aadhaar, surveillance, constitutional protection, India.

I. INTRODUCTION

Contemporary democracies worldwide confront a defining tension: the state's growing capacity and justification for biometric identification clash with individuals' constitutional claims to bodily autonomy and freedom from invasive tracking. India exemplifies this tension acutely. Since 2009, the Unique

Identification Authority of India (UIDAI) has collected fingerprints, iris patterns, and facial photographs from more than 1.3 billion residents through the Aadhaar scheme, ostensibly to deliver welfare benefits, enable financial inclusion, and prevent fraud. Concurrently, India's law enforcement agencies have deployed facial recognition systems to scan CCTV networks, crime databases, and airport terminals, often without explicit statutory authorization or public awareness. While policymakers and technology proponents present these systems as instruments of efficient, inclusive governance, critical constitutional questions remain largely unresolved: Does the extraction and centralization of biometric data inherently violate bodily integrity? Can consent to biometric surrender be "free" when welfare access depends on enrollment? What makes facial recognition qualitatively different from fingerprinting or passport photography?

The Indian Supreme Court's jurisprudence on privacy, especially the 2017 *Puttaswamy* decision recognizing privacy as a fundamental right and explicitly naming bodily integrity as one of privacy's three dimensions, established an important doctrinal foundation. Yet subsequent judgments, particularly the 2018 Aadhaar ruling, revealed deep unresolved tensions. A majority of the Court treated fingerprints and facial scans as observable, external characteristics akin to passport photographs, while a dissenting judge—notably Justice Chandrachud—insisted that biometric data warrants heightened protection because of its permanence, uniqueness, and surveillance potential when networked.

This paper contends that bodily integrity deserves robust, proactive constitutional protection, not merely reactive data-security measures. The current

legislative framework fails to address the fundamental question of when and under what conditions the state may extract biometric information from citizens. The Aadhaar Act permits collection for loosely defined purposes; the Digital Personal Data Protection Act (DPDP Act) emphasizes post-collection security rather than preventing invasive collection. Most critically, facial recognition remains substantially unregulated despite its extraordinary surveillance potential. In a structurally unequal society, these regulatory gaps disproportionately expose the poor, marginalized minorities, and political dissidents to state biometric control, hollowing out the promise of equal citizenship and dignity.

II. THE CONSTITUTIONAL ARCHITECTURE OF BODILY INTEGRITY IN INDIA

2.1. Article 21's Evolution and Privacy's Recognition
The Indian Constitution's Article 21 guarantees that no person shall be "deprived of his life or personal liberty except according to procedure established by law." Unlike many modern constitutions that expressly mention bodily integrity or bodily autonomy, the Indian framers embedded this protection within the expansive language of "personal liberty," leaving courts to elaborate its contours through interpretation. Over decades, the Supreme Court transformed Article 21 from a narrow procedural safeguard into a substantive guardian of fundamental freedoms. The pivotal moment occurred in *Maneka Gandhi v. Union of India* (1978), when the Court held that "procedure established by law" must be "just, fair and reasonable," opening doctrinal space for recognizing unarticulated rights within Article 21's scope [1].

The watershed came in 2017 with *Justice K.S. Puttaswamy (Retd.) v. Union of India*, a nine-judge bench that unanimously declared the right to privacy a fundamental right protected by Article 21[2]. Critically, the judgment articulated privacy as comprising three inseparable dimensions: bodily integrity (inviolability of the physical person and control over biological information), decisional privacy (autonomy in intimate personal choices), and informational privacy (dominion over personal data) [3]. Justice D.Y. Chandrachud's separate concurrence provided particularly forceful language: "the bodily integrity of an individual is sacred. It is the sine qua non of a free and dignified existence. The state,

therefore, cannot encroach upon the inviolability of the physical body of an individual. It is a trespass upon the person to violate their bodily integrity"[4].

2.2. Why Bodily Integrity Matters Constitutionally
Bodily integrity operates as a constitutional value serving three interconnected purposes.

First, it grounds human dignity. The premise is that each person possesses inherent worth that the state must respect. When the state compels extraction of one's biometric markers—converting the living body into data for state archives and algorithmic processing—it risks reducing individuals from autonomous citizens to subjects of surveillance, undermining the dignity that Article 21 protects [5].

Second, bodily integrity upholds autonomy and self-governance. A person who cannot control access to their own body or its characteristics lacks the minimal self-determination that undergirds democratic citizenship. Coerced biometric provision, particularly when tied to welfare access, exploits vulnerability and denies individuals genuine choice [6].

Third, bodily integrity protects liberty understood as freedom from domination. Awareness that facial recognition may identify one's movements through public space, that one's body can be matched against criminal databases, or that biometric profiles enable state categorization produces a chilling effect on political participation, association, and freedom of movement—all constitutionally protected liberties.

2.3. International Frameworks as Comparative Reference

India's reliance on judicial elaboration of Article 21 contrasts with more textually explicit protections elsewhere. The European Union's General Data Protection Regulation (GDPR) explicitly categorizes biometric data as "sensitive personal data" requiring heightened protection, acknowledging that biometric information is qualitatively different from ordinary personal information. The European Court of Human Rights has held that collection and retention of biometric data interferes with Article 8 rights (private life) and requires compelling justification and strict safeguards. South Africa's Constitution expressly protects "bodily and psychological integrity" under

Section 12, and South African courts have interpreted this to encompass state intrusion into bodily autonomy. These frameworks recognize that biometric extraction is not merely a logistical question of data management but a constitutional one touching on personhood and dignity. India's approach, dependent on case-by-case judicial interpretation of Article 21, provides interpretive flexibility but also leaves space for erosion through narrowing judicial constructions—as evidenced by the Aadhaar judgment's treatment of biometric collection as minimally invasive.

III. THE AADHAAR PROGRAMME: SCOPE, JUSTIFICATION, AND BODILY CONCERNS

3.1. The Aadhaar Infrastructure

Launched in 2009 and formalized through the Aadhaar Act of 2016, the Aadhaar scheme represents the world's largest biometric identification system. UIDAI operates a centralized database containing the fingerprints, iris images, and facial photographs of over 1.3 billion Indian residents. The system assigns a 12-digit unique identifier to each enrolled individual, theoretically enabling cross-verification across government and private agencies.

The justifications offered were multifaceted: enabling poor and undocumented citizens to access welfare benefits, targeting subsidies efficiently, promoting financial inclusion by providing identity proof for banking services, and reducing duplicate benefits through deduplication. These objectives align with legitimate state interests in social welfare, fiscal efficiency, and inclusive governance.

3.2. The Practice of Coercion: From Voluntary to Mandatory

Yet in practice, Aadhaar shifted from voluntary to de facto mandatory. While the Act technically permitted voluntary enrollment, the government progressively linked Aadhaar to welfare benefits, income tax filing, mobile phone connections, bank account opening, and utility provisioning. For millions of poor Indians dependent on government transfers, accessing Aadhaar became indispensable, not optional. This "coercive linkage" transformed the constitutional character of biometric provision: what was presented as voluntary became practically compulsory, particularly for those least able to resist—the economically vulnerable.

3.3. Why Biometric Extraction Differs from Routine Identification

Traditional identification (name, address, photograph) differs fundamentally from biometric extraction in four ways.

First, Uniqueness and Permanence:

Fingerprints and iris patterns are unchangeable, lifelong identifiers. Unlike a password that can be reset or a photograph that can age, biometric data remains fixed and unique, creating a permanent, singular link between body and identity.

Second, Surveillance Potential:

Once lodged in centralized databases, biometric data enables rapid, large-scale matching against other databases (criminal records, CCTV footage, welfare rolls), facilitating tracking and profiling impossible with traditional documents.

Third, Bodily Intrusion:

Even if minimally invasive compared to blood draws or DNA extraction, the act of fingerprinting or iris scanning involves state contact with bodily surfaces and biological information, constituting a form of bodily intrusion.

Fourth, informational dignity:

Individuals possess an informational interest in their biometric data distinct from mere observation. The state's capacity to observe one's face does not automatically entitle it to record, store, and process facial images indefinitely. Recognition of this informational interest in bodily characteristics was central to Justice Chandrachud's dissent in the Aadhaar judgment.

IV. FACIAL RECOGNITION: AMPLIFIED SURVEILLANCE INTRUSION

Facial recognition technology introduces surveillance capabilities qualitatively distinct from traditional biometric collection. Unlike fingerprinting or iris scanning (which require active participation), facial images can be captured covertly through CCTV cameras, smartphones, or aerial drones [20]. India's law enforcement agencies—particularly the National Crime Records Bureau (NCRB)—have deployed Automated Facial Recognition Systems (AFRS)

linking CCTV networks with criminal databases, enabling real-time identification of individuals in public spaces. Multiple Indian cities have installed surveillance grids equipped with facial recognition, and airports use the technology for immigration control.

Facial recognition's unique hazards to bodily integrity and freedom include: (1) Pervasive covert capture of facial data without knowledge or consent as individuals move through public space; (2) Real-time mass surveillance enabling continuous tracking rather than episodic identification; (3) Chilling effects on protest, assembly, and movement when citizens know facial recognition may track their public activities; (4) Algorithmic bias affecting women and darker-skinned individuals disproportionately, creating intersecting bodily integrity and equality violations; (5) Mission creep, wherein systems deployed for crime-fighting become tools for political profiling or targeting of minorities.

These features render facial recognition categorically more invasive to bodily integrity than fingerprinting. It transforms the street, the transit platform, and the protest site into spaces where the body becomes the site of automated identification and state recording, even for citizens not suspected of crime.

V. JUDICIAL DOCTRINE AND LEGISLATIVE GAPS

5.1. The Aadhaar Judgment's Unresolved Tensions

The September 2018 Supreme Court judgment on Aadhaar's constitutionality produced three separate opinions, reflecting doctrinal discord. Four judges upheld the Aadhaar Act, holding that biometric collection does not violate bodily integrity because fingerprints and iris scans are externally observable, akin to passport photographs [23]. Justice Chandrachud, while joining the majority on other grounds, filed a distinctive concurrence emphasizing that biometric data deserves heightened protection. He argued that governments must follow a "compelling state interest" test for biometric collection and a "no harm principle," ensuring that biometric data is not used to discriminate or harm individuals or for purposes undisclosed at collection.

The majority's minimalist approach—treating biometrics as observable external characteristics—has been criticized for ignoring the technological and

practical differences between a passport photograph and a permanent, networked, algorithmically searchable biometric database. The majority failed to acknowledge that facial recognition operates differently from human recognition, enabling mass surveillance incompatible with bodily autonomy.

5.2. Legislative Deficits

The Aadhaar Act nominally designates biometric data as "sensitive," yet provides weak protections. It permits collection for loosely defined "welfare schemes" without strict necessity requirements. It grants UIDAI broad, unilateral powers to expand the definition of collectible biometric data, potentially authorizing more invasive collection (blood, DNA) without statutory amendment. It lacks independent oversight mechanisms and provides individuals minimal rights to access, challenge, or delete biometric information.

The Digital Personal Data Protection Act (2023) was intended to establish baseline data protection standards. However, it treats biometric data merely as one category of "sensitive personal data" and focuses on post-collection security rather than preventing invasive collection.

Crucially, the Act exempts government agencies, leaving state-sponsored biometric programs like Aadhaar and facial recognition deployments substantially unregulated.

Facial recognition remains almost entirely unregulated. Unlike the European Union, which has proposed strict regulations on high-risk facial recognition uses, India possesses no dedicated facial recognition statute.

Law enforcement deploys facial recognition systems under generic provisions of the Indian Penal Code and Criminal Procedure Code, without judicial authorization requirements, accuracy standards, or mandatory impact assessments.

VI. TOWARD A BODILY INTEGRITY-CENTERED FRAMEWORK

6.1. Core Constitutional Principles

Given the foregoing analysis, protecting bodily integrity in an age of biometric governance requires five foundational principles:

Principle 1: Compelling Interest and Necessity

Biometric collection must serve demonstrable, compelling state interests achievable through no less invasive means. The state bears the burden of proving necessity, not individuals bearing the burden of proving harm.

Principle 2: Genuine Consent and Alternatives

Consent to biometric surrender must be freely given, informed, purpose-specific, and without coercion through welfare or service access. Individuals refusing biometric collection must retain access to essential services and rights.

Principle 3: Data Minimization and Purpose Limitation

Collection must be limited to what is strictly necessary. Biometric data collected for one purpose cannot be repurposed for mass surveillance or political profiling without fresh legal authorization.

Principle 4: Transparency and Individual Control

Citizens must know what biometric data is held, how it is used, and by whom. Individuals must possess meaningful rights to access, correct, and delete biometric information.

Principle 5: Independent Oversight and Accountability

Deployment of facial recognition and major expansions of biometric collection require statutory authorization following public debate. Judicial authorization should govern investigative use of facial recognition. Independent audits and impact assessments must precede deployment.

6.2. Facial Recognition-Specific Safeguards

Given facial recognition's extraordinary surveillance potential, additional safeguards are essential:

- 1) Statutory authorization for any facial recognition deployment, not mere administrative discretion;
- 2) Judicial warrants for investigative uses, analogous to wiretap authorizations;
- 3) Accuracy standards with public disclosure of error rates, particularly disaggregated by gender and skin tone;
- 4) Prohibition on mass surveillance of public spaces absent extraordinary statutory authorization and regular parliamentary review;

5) Categorical ban on profiling based on protected characteristics (caste, religion, political affiliation);

6) Mandatory impact assessments assessing risks to bodily integrity, privacy, and equality before deployment.

VII. SECURITY, INCLUSION, AND DEMOCRATIC TENSIONS

Governments commonly justify biometric surveillance through security (crime prevention, counterterrorism) and inclusion (welfare access) narratives. These justifications deserve response but cannot override bodily integrity protections.

On security:

Facial recognition's purported crime-fighting benefits are contested empirically. High-profile wrongful arrests based on facial misidentification suggest that algorithmic surveillance creates new security problems while solving old ones. Moreover, once surveillance infrastructure is built, it tends to persist even after security threats diminish, and its use typically expands to new purposes absent strict safeguards. For most legitimate law enforcement, less invasive alternatives exist: targeted surveillance of specific suspects, voluntary offender registries, traditional investigation.

On inclusion:

Aadhaar genuinely enabled millions to access services and financial systems. Yet inclusion need not require mandatory biometric extraction. Governments could provide alternative identity verification pathways for those unwilling to provide biometrics, reducing practical coercion [34]. Treating welfare as a right—rather than conditional on biometric surrender—would be more dignified and constitutional.

VIII. COMPARATIVE CONSTITUTIONAL MODELS

The European Union treats biometric data as categorically sensitive, requiring explicit consent and strict limitation on processing. The GDPR prohibits mass surveillance with facial recognition absent compelling justification, and the European Data Protection Board has effectively restricted its use by law enforcement. South Africa's textually explicit

protection of bodily integrity in Section 12 of its Constitution provides clearer doctrinal foundation than India's reliance on Article 21 interpretation. These models suggest that India should consider explicit legislative recognition of heightened biometric protection, moving beyond reliance on judicial case-by-case elaboration.

IX. RECOMMENDATIONS AND PATHS FORWARD

Legislative:

India should enact a comprehensive Biometric Data Protection Act establishing strict necessity requirements, meaningful consent rules, data minimization principles, individual rights to access and delete biometric data, and independent oversight. A separate Facial Recognition Regulation Act should govern facial recognition deployment, requiring statutory authorization, judicial warrants for investigative use, accuracy standards, prohibition on mass surveillance, and bans on discriminatory profiling.

Judicial:

The Supreme Court should clarify in future decisions that bodily integrity encompasses informational and dignitary dimensions, that coercive biometric extraction violates bodily integrity regardless of minimal physical invasiveness, and that facial recognition raises distinct constitutional concerns warranting heightened protection.

Executive:

The government should impose a moratorium on expanding facial recognition pending independent impact assessments. Transparency requirements should mandate disclosure of facial recognition accuracy rates, retention periods, and demographic bias patterns. Independent audits should assess compliance with purpose limitation and data minimization principles.

X. CONCLUSION

Biometric databases and facial recognition represent a fundamental shift in state capacity to identify, track, and profile citizens. While these technologies offer governance efficiencies and potential social benefits,

they pose unprecedented threats to bodily integrity—the constitutional value protecting dignity, autonomy, and freedom from domination. The Indian Supreme Court's recognition of bodily integrity as a fundamental right component is doctrinally significant. Yet the Aadhaar judgment's narrow conception of biometric intrusion, combined with legislative gaps and facial recognition's regulatory vacuum, leaves bodily integrity inadequately protected.

In India's structurally unequal society, where the poorest depend on state welfare and minorities face disproportionate policing, unregulated biometric surveillance threatens to deepen existing inequalities. The path forward requires treating bodily integrity not as a narrow limit on technology but as foundational constitutional value guiding biometric governance. This demands robust legislation establishing necessity thresholds, genuine consent rules, data minimization principles, and independent oversight. It demands judicial clarification that bodily integrity encompasses informational and dignitary dimensions, particularly in the context of networked, algorithmic surveillance. Most fundamentally, it demands a democratic commitment to the principle that technological power must serve, not subjugate, equal citizens.

REFERENCES

- [1] *Maneka Gandhi v. Union of India*, AIR 1978 SC 597, para. 53.
- [2] *Justice K. S. Puttaswamy (Retd.) v. Union of India*, AIR 2017 SC 4161 (nine-judge bench).
- [3] *Id.*, para. 107.
- [4] *Id.*, Justice D. Y. Chandrachud's separate judgment, para. 75.
- [5] Usha Ramanathan, "Biometrics, Turning a 'Citizen' into a 'Subject,'" *Deccan Herald*, Sept. 30, 2018.
- [6] Apar Gupta and Abhinav Sekhri, "The Mandatory Aadhaar Problem: Coercion and Constitutionality," *Internet Freedom Foundation Blog*, Sept. 2018.