DIGITAL IDENTITY AND BIOMETRICS IN INDIA: GOVERNING PRIVACY AND SECURITY IN THE DIGITAL AGE

Satyam Singh, Research Scholar, Deen Dayal Upadhaya Gorakhpur University, Gorakhpur, Uttar Pradesh

Dr. Ashish Kumar Shukla, Assistant Professor, Deen Dayal Upadhaya Gorakhpur University, Gorakhpur, Uttar Pradesh

ABSTRACT

This article examines the regulation of digital identity and biometric systems in India through the lens of data governance, privacy, and cyber security. It traces the historical development of Aadhaar and the broader 'JAM' architecture, situating these initiatives within a constitutional jurisprudence that recognizes privacy as a fundamental right. It then analyses the principal legal instruments the Information Technology Act, 2000; the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016; the Digital Personal Data Protection Act, 2023; and the 2022 CERT-In directions and discusses how they allocate responsibilities and risks across public and private actors. Against this backdrop, the paper assesses technical and governance challenges in biometric enrolment and authentication, the political economy of direct benefit transfers and financial inclusion, and the rise of facial recognition in public service delivery and law enforcement. Drawing on international standards such as NIST SP 800-63-4 and World Bank ID4D guidance, the article proposes a policy agenda for rights-preserving digital identity, including risk-based assurance levels, formal prohibitions on open-ended surveillance, independent oversight and auditability, stronger breach notification and redress, and inclusive design to reduce exclusion errors. The analysis concludes that India can harness the developmental benefits of digital identity only by embedding privacy-by-design and security-by-default into institutional practice, supported by legal safeguards and robust accountability mechanisms.

Introduction

India's transformation into a digitally enabled economy has been accompanied by an equally profound transformation in the way individuals are identified, authenticated, and given access to services. Digital identity whether established through a biometric database like Aadhaar, a mobile-based credential, or a combination of identity tokens has become the primary gateway to a wide range of governmental, financial, and commercial services. In its simplest sense, a digital identity is an electronic representation of an individual's attributes such as name, date of birth, photograph, biometrics, or other identifiers that enables a system to verify who they are. In practice, digital identity systems in India extend well beyond a static representation of identity; they operate as dynamic infrastructures enabling real-time authentication, often in remote and automated ways. This evolution is rooted in a vision of improving efficiency, transparency, and inclusivity in service delivery, but it simultaneously raises new and complex challenges concerning privacy, cybersecurity, and governance.

At the heart of India's identity revolution is the Aadhaar programme, the world's largest biometric identification system. Managed by the Unique Identification Authority of India (UIDAI), Aadhaar assigns a unique 12-digit number to residents based on the collection of demographic information and biometric data, including fingerprints, iris scans, and facial photographs. This system has been integrated into what is often described as the "JAM" trinity - Jan Dhan Yojana bank accounts, Aadhaar numbers, and mobile phones which collectively form a backbone for delivering subsidies, benefits, and financial services. Through mechanisms such as Direct Benefit Transfer, subsidies for cooking gas, food grains, and other welfare benefits are routed directly into beneficiaries' bank accounts after Aadhaar-based authentication. In policy terms, the JAM architecture is seen as a tool for reducing leakages, eliminating ghost beneficiaries, and improving the accuracy of targeting. However, these same characteristics - centralisation of data, mass enrolment of citizens, and integration into essential services also concentrate risks in ways that traditional, decentralised identity documents did not.

Biometric systems, such as those used in Aadhaar, rely on unique physiological or behavioural traits to establish identity. In theory, biometrics are harder to forge than paper documents and can provide a higher level of assurance in remote transactions. However, biometric data is not a secret. It is inherently public in the sense that fingerprints, faces, and irises are exposed in everyday interactions. Once compromised, biometric identifiers cannot be "reissued" in the

way a password or card can. This permanence makes biometric breaches particularly dangerous. Moreover, biometric authentication can fail for legitimate users due to factors such as worn fingerprints in manual labourers, poor connectivity in rural areas, or faulty sensors, leading to exclusion from critical services. Such exclusion errors, while statistically small in percentage terms, can have severe real-world consequences, particularly for economically vulnerable individuals who depend on timely access to subsidies or rations.

The concept of data governance is central to understanding how such identity systems can be made both effective and rights-preserving. Data governance refers to the framework of laws, policies, technical standards, and institutional practices that determine how data is collected, processed, stored, shared, and deleted. In the Indian context, multiple statutory instruments form the legal scaffolding for digital identity governance. The Information Technology Act, 2000, provides the overarching legal basis for electronic transactions and certain data protection obligations, though its scope and enforcement mechanisms are limited. The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, sets out the legal framework specific to Aadhaar, prescribing who can collect and use Aadhaar data, under what conditions, and with what safeguards. More recently, the Digital Personal Data Protection Act, 2023, has introduced a generalised regime for the processing of personal data, applicable to both public and private actors, with consent, purpose limitation, and data minimisation as core principles. In the cybersecurity domain, the Indian Computer Emergency Response Team (CERT-In) has issued directions—most recently in 2022—that impose specific security incident reporting timelines, log retention requirements, and obligations on intermediaries and service providers to strengthen the overall cyber-resilience of critical systems.

Privacy, in this setting, operates as both a constitutional right and a practical necessity for maintaining public trust. The Supreme Court's landmark judgment in Justice K.S. Puttaswamy v. Union of India (2017) elevated privacy to the status of a fundamental right under Article 21 of the Constitution, meaning that any infringement must meet the tests of legality, necessity, and proportionality. Justice Chandrachud's powerful dissent critiqued structural issues such as surveillance potential and the Money Bill passage strategy, dubbing it a "fraud on the Constitution"

In the Aadhaar context, this has meant that certain forms of mandatory linking such as for mobile SIM cards have been struck down, while others such as for welfare subsidies—have

been upheld on the grounds of targeted benefits and public interest. Yet privacy is not only a matter of limiting unlawful state intrusion; it also involves preventing misuse by private actors, unauthorised access, and data breaches. In a world where authentication logs, location data, and transaction histories can be mined for profiling or surveillance, strong privacy safeguards must be built into the technical architecture itself, rather than treated as an afterthought.

Cyber security underpins the very trustworthiness of digital identity systems. A breach of a central biometric database, or of an authentication API, could enable identity theft at an unprecedented scale, compromise sensitive records, and undermine confidence in government and financial services. Cyber security in this context encompasses both preventive measures such as encryption, multi-factor authentication, intrusion detection, and secure coding practices and reactive measures, such as timely breach notification, incident response, and recovery. International standards such as NIST Special Publication 800-63-4, which sets guidelines for digital identity assurance levels, emphasise a risk-based approach, where higher-risk transactions require stronger authentication factors and more robust verification processes. Applying such standards to India's context would mean distinguishing between low-assurance uses of Aadhaar (e.g., accessing non-sensitive information) and high-assurance uses (e.g., authorising large financial transfers), and tailoring security controls accordingly.

The governance challenges are not limited to technology. They also involve institutional arrangements, political economy, and social equity. The integration of digital identity into welfare delivery has reconfigured the relationships between citizens, the state, and intermediaries. By making identity verification a prerequisite for receiving benefits, the system can, in principle, reduce fraud, but it also places the burden of technological failure on the individual, who may have little recourse when authentication fails. Similarly, as facial recognition technologies are increasingly deployed in public spaces for law enforcement or crowd management, questions arise about the proportionality of such measures, the potential for mass surveillance, and the adequacy of consent in environments where participation is not truly voluntary.

From a comparative perspective, guidance from the World Bank's Identification for Development (ID4D) programme highlights principles of inclusion, design, and governance as essential for sustainable digital identity systems. Inclusion requires that all individuals regardless of socio-economic status, geography, or digital literacy can obtain and use a digital identity without undue barriers. Design entails embedding privacy-by-design and security-by-

default principles into the technical architecture, ensuring interoperability while preventing excessive data collection. Governance requires clear legal frameworks, independent oversight bodies, and mechanisms for accountability, such as regular audits, grievance redress systems, and public transparency reports.

Ultimately, India's trajectory in regulating digital identity and biometric systems will determine not only the efficiency of service delivery but also the strength of democratic freedoms in a digital age. The central challenge is to reconcile the developmental potential of identity-linked digitisation with the constitutional imperative to protect individual rights. This requires moving beyond a binary debate of "Aadhaar good" or "Aadhaar bad" and towards a nuanced understanding of risk, proportionality, and context. It calls for a multi-layered governance model that differentiates assurance levels by risk, prohibits open-ended surveillance, mandates breach notifications, and institutionalises independent oversight. Only through such an integrated approach where technological architecture, legal safeguards, and institutional accountability reinforce each other can India ensure that its digital identity systems are both effective and respectful of the rights and dignity of every individual.

India's rapid digitisation has made digital identity a cornerstone of service delivery, payments, and welfare administration. From subsidies delivered through Direct Benefit Transfer (DBT) to e-KYC for financial services and airport travel via Digi Yatra, authentication mediated by Aadhaar and other biometric systems is increasingly woven into everyday life. The policy premise is compelling: accurate identification deters fraud, improves targeting, and reduces leakage. Yet the very attributes that make biometric identity powerful—centralisation, scale, and persistence also magnify risks: privacy intrusions, mission creep, cybersecurity incidents, and exclusion of legitimate beneficiaries when authentication fails.

This article analyses digital identity and biometrics in India as a problem of data governance. It proceeds on three assumptions. First, the right to privacy is a constitutional constraint on state and private power, requiring necessity and proportionality in any intrusion. Second, cybersecurity is a precondition for trustworthy identity; weak security translates into weak rights. Third, governance must be risk-based and evidence-driven, recognising that different services warrant different identity assurance levels. On this basis, we evaluate the statutory framework and propose reforms aligned with international best practice.

Historical Development of Digital Identity in India

India's contemporary digital identity trajectory crystallised with the launch of the Unique Identification Authority of India (UIDAI) and the Aadhaar programme in 2009, culminating in the Aadhaar Act, 2016. In parallel, the 'JAM' trinity - Jan Dhan bank accounts, Aadhaar numbers, and mobile connectivity underpinned the expansion of DBT across schemes. The Supreme Court's privacy decision in 2017 recognised privacy as a fundamental right, and the 2018 Aadhaar verdict upheld the core of the scheme while curtailing some uses. Together, these milestones shaped the institutional field within which biometric identity now operates.

Administrative use cases proliferated: subsidies, pensions, SIM registration, e-KYC, and more recently, paperless air travel through Digi Yatra. Each use case embeds policy choices about who must identify, how often, and with what safeguards. Over time, those choices have shifted from one-time verification to continuous authentication, raising questions about proportionality and purpose limitation.

Conceptual Foundations: Digital Identity, Biometrics, and Data Governance

Digital identity refers to the set of attributes used to uniquely represent a person in a digital context, supported by processes of identity proofing (enrolment), authentication, and federation. Biometrics such as fingerprints, iris scans, and facial images are a class of identifiers that are (largely) immutable and probabilistic by nature. As such, they require careful calibration to balance false match and false non-match rates, and to manage lifecycle risks like template aging and sensor variability.

From a data-governance perspective, the core design choices concern

(a) Assurance levels for proofing and authentication;

(b) Centralisation versus federation of credentials and logs;

(c) Consent and legitimate-use grounds;

(d) Retention, purpose limitation, and data minimisation; and

(e) Accountability audits, transparency, and user redress.

International standards, such as NIST SP 800-63-4, formalise a risk-based approach that decouples identity assurance from authentication assurance and emphasises privacy-enhancing technologies, including unlinkability where feasible.

Legal Provisions and Barriers

Four legal pillars frame digital identity in India. First, the Information Technology Act, 2000 (as amended) establishes offences and remedies for cyber incidents and imposes liability on body corporates for failure to implement reasonable security practices (e.g., Sections 43A, 66C, 72A). Second, the Aadhaar Act, 2016 provides the statutory basis for unique identification and authentication, with Section 7 enabling Aadhaar-based delivery of subsidies, benefits, and services. Third, the Digital Personal Data Protection Act, 2023 (DPDP Act) codifies lawful bases for processing digital personal data, recognises data principal rights, and creates a complaints pathway via the Data Protection Board. Fourth, CERT-In's 2022 directions mandate 6-hour breach reporting and 180-day log retention in India, with implications for data localisation and privacy.

Judicially, the Supreme Court's nine-judge bench in 2017 affirmed privacy as a fundamental right and articulated a proportionality test. In 2018, the Court upheld the constitutionality of the Aadhaar Act, while invalidating certain uses (such as mandatory linkage for mobile phones and private-sector authentication without adequate law). These rulings require the State to anchor identity programmes in clear statutory authority, necessity, and specific safeguards, including data minimisation and purpose limitation.

Barriers persist. The DPDP Act's broad 'legitimate uses' and exemptions for State functions risk diluting consent; the CERT-In directions' log-retention and localisation features complicate privacy-by-design; and fragmented sectoral rules create compliance uncertainty. Moreover, redress mechanisms for authentication failures remain patchy, and compensation for wrongful denial of entitlements is rare.

Environmental, Technical, and Governance Challenges

At population scale, biometric systems confront accuracy, availability, and adversarial risks. Environmental conditions (heat, humidity, manual labour), sensor quality, and template drift can elevate false non-match rates, producing welfare exclusion when authentication is a hard

gate. Conversely, low match thresholds raise false positives, especially in one-to-many identification (e.g., watchlists). Robustness requires liveness detection, calibrated thresholds by context, and fallback mechanisms (OTP, human-in-the-loop, offline tokens).

Cyber security poses systemic risk. Central repositories and authentication logs can be high-value targets; breaches involving biometric templates are practically irreversible. Regular third-party audits, key management hygiene, cryptographic binding of transactions, and minimal retention of transaction metadata are essential. Breach notification timelines must align with rapid containment, and affected users should have clear rights to remedies and re-issuance of credentials where feasible (e.g., revocation and re-binding of virtual IDs).

Governance challenges include vendor lock-in, opaque procurement, and limited independent testing. Transparent accuracy reporting across demographic subgroups, and public release of audit summaries, can mitigate performance and fairness concerns. Finally, impact assessments should explicitly model harm both inclusion errors (fraud) and exclusion errors (denial) so that design optimises social welfare rather than mere throughput.

Political Economy and Socio-economic Angles

Supporters argue that Aadhaar-enabled DBT has reduced leakage and improved targeting across LPG, pensions, and scholarships. Government assessments report substantial savings and near-universal seeding, while independent evaluations show mixed effects and urge caution in attributing all savings to identity de-duplication. The truth likely lies in between: identity platforms are necessary but not sufficient administrative capacity, grievance redress, and market structure matter as much.

At the same time, field research and audits document exclusion stemming from authentication failures, connectivity outages, or demographic mismatch. The welfare cost of a false reject can be severe for low-income households, suggesting a design principle of ‘no denial at first instance’ with post-hoc verification and audit trails. These trade-offs are not merely technical; they reflect distributive choices about who bears the cost of errors.

Cyber security and Risk Management

The rise of face recognition in public safety and travel has intensified concerns about surveillance and cyber security. In Delhi and other cities, media and civil-society reports

describe deployments with low match thresholds and limited transparency. Large biometric repositories—including those managed by private contractors have suffered misconfigurations and data leaks. Risk management must therefore prioritise data minimisation, encryption in transit and at rest, strict access control, and independent red-team testing.

Standards can help. NIST SP 800-63-4 promotes risk-based identity assurance, phishing-resistant authenticators, and privacy-enhancing design such as unlinkable federated assertions. Applying these principles in India would entail context-specific thresholds, tiered assurance by service criticality, and auditable logs with retention caps and purpose limitation. Sector regulators should reference such norms to harmonise expectations.

Societal Benefits and Harms

Digital identity can streamline access to public goods banking, subsidies, mobility and reduce documentary burdens for migrants and the unbanked. For beneficiaries, predictable cash transfers and simplified KYC represent meaningful gains. Yet these benefits must be measured alongside dignitary harms and risks of profiling when identity systems are repurposed for surveillance or social sorting. Dignity-preserving design demands voluntariness where feasible, narrowly tailored mandates, and effective, low-friction redress.

Public trust hinges on transparency. Publishing authentication success and failure rates disaggregated by region and demographic attributes, explaining threshold choices, and documenting corrective action plans can counter information asymmetries. Trust also requires restraint for example, express statutory limits on real-time, bulk facial recognition in public spaces absent judicial authorization and necessity.

International Benchmarks and Best Practices

International guidance underscores that no single authentication modality suits every context. The World Bank's ID4D initiative urges risk-based selection of biometrics, attention to lifecycle costs, and strong legal safeguards for privacy and redress. Experience across countries shows that centralised ID can coexist with privacy if supported by independent regulators, purpose limitation, and data minimisation. A comparative lens also cautions against expansive face recognition without demonstrable necessity and proportionate safeguards.

For India, aligning with best practice implies formalising risk assessments, adopting multi-

factor options (including possession-based tokens) in lieu of rigid biometric gates, and institutionalising external certification of identity systems and algorithms. Harmonised standards across sectors would reduce compliance friction while raising the floor on privacy and security.

Conclusions and Suggestions

Digital identity and biometric systems are now embedded in India's administrative state. The challenge is not whether to use them, but how. A principled path forward requires tightening legal safeguards, engineering for resilience and inclusion, and subjecting deployments to independent oversight. The following steps would, together, advance a rights-preserving architecture:

- Enact explicit statutory limits and oversight for real-time, public-space facial recognition, mandating necessity, proportionality, and prior judicial authorization.
- Operationalize the DPDP Act with sector-specific rules for high-risk processing (biometrics), including stricter retention limits, impact assessments, and mandatory breach notification with user redress.
- Implement risk-based assurance levels modelled on NIST SP 800-63-4; require fallback mechanisms and 'no denial at first instance' for essential services.
- Publish disaggregated authentication metrics and independent audit summaries; accredit labs and mandate periodic red-team exercises.
- Limit and better target CERT-In log-retention mandates; ensure due process and transparency for requests while preserving rapid incident response.
- Promote federated and privacy-enhancing designs (tokenisation, virtual IDs, unlinkable assertions) to reduce correlation risk across domains.
- Strengthen grievance redress and compensation for wrongful denial; assign clear liability across the identity value chain, including vendors.

References

1. Dixon, P. (2018). *A failure to "do no harm" – India's Aadhaar biometric ID program*. *World Privacy Forum*. Retrieved from https://worldprivacyforum.org/posts/6893/

2. Solomon, B. (2018, September 28). Digital IDs are more dangerous than you think. *WIRED*. Retrieved from https://www.wired.com/story/digital-ids-are-more-dangerous-than-you-think/

3. Centre for Internet and Society. (2018). *Digital ID evaluation framework – India cases*. Retrieved from https://digitalid.design/evaluation-framework-case-studies/india.html

4. Panigrahi, S. (2022). Marginalized Aadhaar: India's Aadhaar biometric ID and mass surveillance. *ACM Interactions*, 29(2). Retrieved from https://interactions.acm.org/archive/view/march-april-2022/marginalizedaadhaar

5. Privacy International. (2019). Exclusion by design: How national ID systems make social protection inaccessible to vulnerable populations. Retrieved from https://privacyinternational.org/case-study/4698/id-systems-analysed-aadhaar

6. Solomon, B. (2018, February 13). Indian Aadhaar issues. *WIRED*. Retrieved from https://www.wired.com/beyond-the-beyond/2018/02/indian-aadhaar-issues/

7. Trilegal. (2022). *2022 CERT-In Directions on Reporting Cyber Incidents*. Retrieved from https://trilegal.com/wp-content/uploads/2022/05/2022-CERT-In-Directions-on-Reporting-Cyber-Incidents-1.pdf

8. Time. (2018, September 27). The world's largest biometric identification system survived a Supreme Court challenge in India. *Time*. Retrieved from https://time.com/5388257/india-aadhaar-biometric-identification/

9. Sundararajan, V., & Narayanan, A. (2022). Aadhaar structure security vulnerabilities. *International Association for Cryptologic Research (IACR)*. Retrieved from https://www.iacr.org/cryptodb/data/paper.php?pubkey=3971724

10. Government of India. (2018). Government savings via JAM (SPRF). *Press Information Bureau*. Retrieved from https://pib.gov.in/PressReleasePage.aspx?PRID=1535673

11. Ministry of Electronics and Information Technology. (2023). *The Digital Personal Data Protection Act, 2023 (No. 22 of 2023)*. Retrieved from https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

12. Unique Identification Authority of India. (2016). *Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016*. Retrieved from https://uidai.gov.in/images/Aadhaar_Act_2016_as_amended.pdf

13. National Institute of Standards and Technology. (2025). *NIST Special Publication 800-63-4 - Digital Identity Guidelines*. Retrieved from https://pages.nist.gov/800-63-4/sp800-63.html

14. Solomon, B. (2024, July 15). India's dodgy mass surveillance project should concern us all. *WIRED*. Retrieved from https://www.wired.com/story/india-aadhaar-biometrics-privacy/

15. Chandrachud, D. Y. (2018). Dissenting opinion in *K.S. Puttaswamy v. Union of India*, Writ Petition (Civil) No. 494 of 2012. *Supreme Court of India*. Retrieved from https://main.sci.gov.in/jonew/judis/48941.pdf

16. Puttaswamy, K. S. (2017). *K.S. Puttaswamy v. Union of India*, Writ Petition (Civil) No. 494 of 2012. *Supreme Court of India*. Retrieved from https://main.sci.gov.in/jonew/judis/48941.pdf