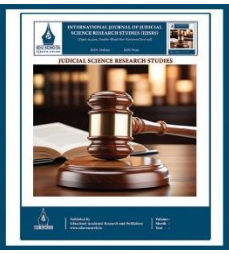
INTERNATIONAL JOURNAL OF JUDICIAL SCIENCE RESEARCH STUDIES (IJJSRS)
(Open Access, Double-Blind Peer Reviewed Journal)
ISSN Online: 3049-0618 ISSN Print:



The Legal Architecture Of Digital Public Infrastructures: Consent, Accountability, And Data Sovereignty In India's Aadhaar And UPI Systems

Simi John

Assistant Professor, Department of Law, Marian College Autonomous, Kuttikkanam, Peermade, Idukki, Kerala, India.

Article information

Received: 5th August 2025
Received in revised form:18th September 2025
Accepted: 27th October 2025
Available online: 21st November 2025

Volume: 2
Issue: 4
DOI: https://doi.org/10.5281/zenodo.17668992

Abstract

Digital Public Infrastructures (DPIs) represent a fundamental transformation in state-citizen interactions, with India's Aadhaar biometric identification system and Unified Payments Interface (UPI) serving as paradigmatic examples. This paper examines the legal architecture governing these systems through the triadic framework of consent, accountability, and data sovereignty. The analysis reveals critical tensions between technological innovation and rights protection, particularly following the Supreme Court's 2018 Puttaswamy judgment and the enactment of the Digital Personal Data Protection Act (DPDPA), 2023. Through doctrinal analysis and comparative evaluation, this paper demonstrates that while India has constructed a sophisticated legal framework for DPIs, significant gaps persist in consent mechanisms, accountability structures, and sovereignty protection. The paper argues that the current legal regime, though progressive, requires strengthening through enhanced institutional oversight, clearer data localization mandates, and robust enforcement mechanisms. These findings contribute to understanding how emerging democracies can balance digital inclusion with fundamental rights protection in the era of data-driven governance.

Keywords: - Digital Public Infrastructure, Aadhaar, UPI, Consent Framework, Data Sovereignty, Accountability Mechanisms, DPDPA 2023

I. INTRODUCTION

The digitalization of state functions represents one of the most significant transformations in contemporary governance. India's Digital Public Infrastructure (DPI), comprising the Aadhaar biometric identification system and the Unified Payments Interface (UPI), exemplifies this transformation at unprecedented scale. With over 1.38 billion Aadhaar enrollments and 83 billion UPI transactions annually, these systems have fundamentally restructured the relationship between state, citizen, and market (National Payments Corporation of India , 2024).

The legal architecture governing these systems must navigate complex tensions between technological efficiency and fundamental rights protection. The Supreme Court's landmark recognition of privacy as a fundamental right in (Justice K.S. Puttaswamy v. Union of India ,2017) established new constitutional parameters for data governance. Subsequently, the 2018 Aadhaar judgment and the (Digital Personal Data Protection Act , 2023), have created a multilayered legal framework that attempts to reconcile innovation with rights protectio

This paper examines three critical dimensions of this legal architecture: consent mechanisms, accountability structures, and data sovereignty frameworks. These dimensions are not merely technical considerations but represent fundamental questions about state power, individual autonomy, and national sovereignty in the digital age. The research question guiding this analysis is: How does India's legal framework for DPIs balance technological efficiency with the protection of consent, accountability, and data sovereignty, and what gaps or tensions persist in this architecture?

The significance of this inquiry extends beyond India's borders. As the "India Stack" model gains international attention as a blueprint for developing economies, understanding its legal foundations becomes crucial for global digital governance

discourse (Jiang & Hariharan, 2024). This paper contributes to this understanding by providing a comprehensive doctrinal analysis of India's DPI legal regime, identifying structural strengths and persistent vulnerabilities.

II. THEORETICAL FRAMEWORK AND CONCEPTUAL FOUNDATIONS

The legal architecture of DPIs must be understood through the intersection of multiple theoretical frameworks: privacy law, administrative law, and sovereignty theory. This section establishes the conceptual foundations for analyzing India's DPI regime.

2.1. Privacy as a Fundamental Right

The Puttaswamy judgment (2017) elevated privacy to constitutional status, establishing a three-pronged test for legitimate privacy restrictions:

- Existence of a law,
- Legitimate state interest
- Proportionality (Justice K.S. Puttaswamy v. Union of India, 2017).

This framework creates constitutional parameters within which all data processing activities, including those under DPIs, must operate. The judgment explicitly recognized informational privacy, bodily privacy, and decisional autonomy as protected dimensions.

The proportionality test, borrowed from European jurisprudence, requires that state interference with privacy rights be both necessary and proportionate to the objective sought. This test has become the cornerstone for evaluating the constitutionality of data collection and processing under both Aadhaar and UPI systems.

2.2. Consent Theory in Digital Contexts

Consent in digital ecosystems presents unique challenges. Traditional contract law notions of informed, voluntary consent often break down when dealing with complex technological systems and asymmetric power relationships (Solove, 2013). The DPDPA 2023 attempts to address these challenges through provisions requiring "free, specific, informed and unambiguous" consent (Digital Personal Data Protection Act, 2023), Section 6.

However, the concept of "consent" in the context of state-provided essential services raises fundamental questions about voluntariness. When Aadhaar becomes necessary for welfare benefits or when UPI becomes the dominant payment mechanism, the boundary between consent and compulsion blurs.

2.3. Accountability in Administrative State

Accountability mechanisms in administrative law traditionally encompass three dimensions: transparency (information disclosure), participation (stakeholder involvement), and remediation (grievance redress). In the context of DPIs, these dimensions must extend to algorithmic accountability, data breach notification, and institutional oversight (Bovens, 2007).

The DPDPA 2023 introduces the concept of "accountability" as a core principle, requiring data fiduciaries to implement appropriate technical and organizational measures (Digital Personal Data Protection Act, 2023), Section 8. However, the operationalization of this principle remains contested.

2.4. Data Sovereignty and National Interest

Data sovereignty refers to the principle that data generated within a nation's borders should be subject to that nation's laws and governance structures. India's approach to data sovereignty reflects both economic nationalism and security concerns, manifesting in data localization requirements and restrictions on cross-border data transfers (Jiang, 2024).

The intersection of data sovereignty with international trade obligations creates complex legal tensions. India's evolving position on data flows—moving from strict localization mandates to more nuanced, sector-specific approaches—reflects ongoing negotiation of these tensions.

III. AADHAAR: LEGAL ARCHITECTURE AND CONSENT MECHANISMS

3.1. Legislative Framework

The Aadhaar Act, 2016, provides the primary legal foundation for India's biometric identification system. The Act establishes the Unique Identification Authority of India (UIDAI) as the governing body and creates a framework for enrollment, authentication, and data protection (Aadhaar Act, 2016).

The Act's passage as a "Money Bill," avoiding Rajya Sabha scrutiny, has been subject to constitutional challenge. While the Supreme Court upheld this procedure, Justice Chandrachud's dissent highlighted concerns about circumventing legislative deliberation (Justice K.S. Puttaswamy v. Union of India, 2018).

3.2. The Constitutional Validity Verdict (2018)

The Supreme Court's 2018 judgment in Justice K.S. Puttaswamy v. Union of India represents the most comprehensive judicial examination of Aadhaar's legal architecture. The Court upheld the Act's core provisions while striking down several elements:

3.2.1. Upheld Provisions:

- Section 7: Mandatory Aadhaar for government subsidies and benefits

- Core enrollment and authentication mechanisms
- UIDAI's institutional structure

3.2.2. Struck Down/Modified Provisions:

- Section 57: Prohibited private sector mandatory use of Aadhaar
- Section 33(2): Removed national security exception allowing disclosure without court order
- Regulation 26(c): Prohibited indefinite metadata storage
- Banking and telecom linking requirements under separate laws

The judgment applied the proportionality test, finding that while Aadhaar serves legitimate state interests (welfare delivery, subsidy targeting), certain provisions exceeded proportionate means.

3.3. Consent Architecture Under Aadhaar

The Aadhaar Act's consent framework operates on multiple levels:

Enrollment Consent: Section 3 establishes enrollment as "voluntary," yet practical compulsion arises when Aadhaar becomes necessary for essential services. The Supreme Court addressed this paradox by limiting mandatory Aadhaar to Section 7 benefits while prohibiting private sector compulsion.

Authentication Consent: Section 8 requires requesting entities to obtain explicit consent before authentication. The 2024 amendments strengthened this provision, mandating that consent be:

(1) informed, (2) specific to purpose, (3) accompanied by alternatives notice, and (4) freely revocable (Aadhaar Amendment Regulations, 2024).

Consent Manager Framework: The DPDPA 2023 introduces "Consent Managers"—intermediaries registered with the Data Protection Board who facilitate consent management on behalf of individuals. This architecture, borrowed from India's Account Aggregator framework, represents an innovative approach to digital consent (Digital Personal Data Protection Act, 2023), Section 6(8).

Despite these provisions, implementation challenges persist. Field studies document instances where service providers position Aadhaar as the default option without adequately informing citizens of alternatives, creating a gap between legal standards and practical reality (Privacy International, 2018).

3.4. Accountability Mechanisms

The Aadhaar Act establishes several accountability mechanisms:

Institutional Accountability: The UIDAI operates under the oversight of the Ministry of Electronics and Information Technology (MeitY). However, Justice Chandrachud's dissent highlighted the absence of an independent monitoring authority, arguing that UIDAI's dual role as operator and regulator creates accountability deficits (Justice K.S. Puttaswamy v. Union of India, 2018).

Data Security Obligations: Section 29 mandates security protocols for handling Aadhaar data. The 2019 regulations require biometric data encryption, restricted access protocols, and audit trails. However, documented data breaches have raised questions about enforcement effectiveness.

Penalty Framework: Section 47 establishes civil and criminal penalties for violations. However, the absence of clear enforcement procedures and limited prosecutions have undermined deterrent effects.

Redress Mechanisms: Section 32 establishes grievance redress processes, but critics argue these mechanisms lack independence and accessibility, particularly for marginalized populations who form Aadhaar's primary beneficiaries.

The DPDPA 2023 enhances accountability through mandatory breach notification requirements and establishment of the Data Protection Board, though its full implementation awaits notification of rules (Digital Personal Data Protection Act, 2023), Sections 18-19.

IV. UPI: REGULATORY FRAMEWORK AND OPERATIONAL ACCOUNTABILITY

4.1. Institutional and Legal Structure

Unlike Aadhaar, UPI lacks dedicated primary legislation. Instead, its legal framework derives from multiple sources:

- Payment and Settlement Systems Act, 2007: Provides foundational authority for digital payment systems
- RBI regulations: Multiple circulars governing UPI operations
- NPCI guidelines: Operational circulars issued by the National Payments Corporation of India
- DPDPA 2023: Governs personal data processing in UPI transactions

This fragmented legal architecture creates both flexibility and uncertainty. The absence of dedicated legislation means UPI governance relies heavily on regulatory circulars and industry self-regulation.

4.2. The National Payments Corporation of India

NPCI, established as a not-for-profit company under Section 8 of the Companies Act, operates UPI infrastructure. This hybrid public-private model raises accountability questions. While NPCI is industry-owned (by banks), it performs quasi-public functions in operating national payment infrastructure.

The legal status of NPCI—neither purely governmental nor purely private—creates ambiguities regarding transparency obligations, public accountability, and judicial review. Recent scholarship argues for clearer legislative definition of NPCI's status and obligations (Hariharan & Natarajan, 2024).

4.3. Consent Mechanisms in UPI

UPI's consent architecture operates differently from Aadhaar:

Transaction Consent: Each UPI transaction requires explicit authentication through PIN or biometric verification. This transaction-level consent provides granular control but also creates friction.

Data Sharing Consent: The NPCI guidelines mandate explicit user consent before data sharing with third parties. However, the 2025 amendments strengthen these requirements, mandating that consent be opt-in rather than default (NPCI Circular 220, 2025).

Numeric UPI ID Consent: Recent regulations require explicit consent for seeding and porting UPI numbers, with mandatory provision of alternatives. This addresses earlier concerns about forced adoption (NPCI Guidelines, 2025).

The integration of UPI with the Account Aggregator framework creates additional consent layers, allowing users to control financial data sharing across institutions through standardized consent artifacts.

4.4. Accountability and Security Framework

Recent NPCI circulars have significantly enhanced UPI's accountability framework:

API Security Guidelines (OC-215/2025-26): Mandate comprehensive security controls, including rate limiting, input validation, and audit logging. Non-compliance results in API access restrictions and penalties (NPCI, 2025).

Transaction Limits and Monitoring: The 2025 amendments impose strict limits on API calls (50 balance enquiries, 25 account listings per day per app) to prevent excessive data extraction and system abuse.

Chargeback and Dispute Resolution: Updated procedures mandate automatic acceptance/rejection of chargebacks and establish clear timelines for resolution. The "4-hour rule" requires issue resolution within four hours of reporting.

Breach Notification: PSPs must report breaches to NPCI immediately, with monthly reporting of locally settled UPI numbers during system delays, ensuring transparency and accountability.

These mechanisms represent significant advances in operational accountability. However, questions persist about NPCI's own accountability, particularly regarding transparency in decision-making and stakeholder participation.

V. DATA SOVEREIGNTY AND CROSS-BORDER DATA FLOWS

5.1. India's Data Localization Approach

India's approach to data sovereignty has evolved from broad localization proposals to sector-specific requirements:

(RBI Mandate ,2018): Requires all payment system operators to store payment data exclusively within India. This mandate directly impacts UPI operations and represents one of the strictest financial data localization requirements globally.

Aadhaar Data Localization: The Aadhaar Act prohibits storage of Core Biometric Information outside India (Aadhaar Act, 2016), Section 29. Authentication logs must also be stored domestically.

DPDPA Framework: The DPDPA 2023 does not mandate blanket data localization but grants the government power to notify "restricted countries" to which data transfers are prohibited. This creates a negative list approach, maintaining flexibility while preserving sovereignty concerns (Digital Personal Data Protection Act, 2023), Section 16.

The evolution from blanket localization to sector-specific and restricted-country approaches reflects India's attempt to balance sovereignty concerns with economic pragmatism and international trade obligations.

5.2. Theoretical Justifications and Critiques

Proponents of data localization advance several justifications:

- Law Enforcement Access: Localization facilitates timely law enforcement access to data without depending on foreign legal assistance treaties.
- Economic Development: Requiring local data storage stimulates domestic data center industry and creates technology jobs.
- National Security: Preventing foreign access to citizens' sensitive data protects against surveillance and potential weaponization.
- Digital Sovereignty: Asserting regulatory control over data generated within national borders exercises legitimate sovereign prerogatives.

5.3. Critics counter with several concerns:

Economic Costs: Localization requirements impose significant infrastructure costs, particularly on startups and SMEs, potentially hindering digital economy growth.

Trade Tensions: Strict localization conflicts with international trade agreements and free data flow principles, risking retaliatory measures.

Security Paradoxes: Concentrating sensitive data in domestic servers may actually increase security vulnerabilities if domestic infrastructure is less sophisticated than global alternatives.

Surveillance Risks: Localization facilitates state surveillance by ensuring all data remains within governmental reach, potentially undermining the privacy protections the framework ostensibly serves.

5.4. Comparative Analysis: India, EU, and China

Table 1 compares India's data sovereignty approach with the European Union's GDPR and China's Cybersecurity Law:

Table 1. Comparative Data Sovereignty Frameworks

Dimension	India (DPDPA 2023)	EU (GDPR)	China (CSL 2017)
Localization Mandate	Sector-specific; negative list for transfers	No mandatory localization; adequacy decisions for transfers	Mandatory for critical information infrastructure operators
Legal Basis for Transfer	Government notification; restricted countries	Adequacy assessment by European Commission; Standard Contractual Clauses	Security review by Cyberspace Administration
Individual Rights	Strong consent requirements; data principal rights	Robust individual rights; right to be forgotten; data portability	Limited individual rights; national security primacy
Regulatory Authority	Data Protection Board (to be operationalized)	National Data Protection Authorities; EDPB coordination	Cyberspace Administration of China; centralized control
Enforcement Mechanism	Penalties up to ₹250 crores; enforcement pending	Fines up to 4% of global revenue; strong enforcement record	Severe penalties including business suspension; party-state enforcement

This comparative analysis reveals India's hybrid approach: borrowing consent-centric frameworks from GDPR while maintaining sovereignty-focused localization similar to China, yet attempting to preserve democratic accountability mechanisms.

5.5. The Tension Between Sovereignty and Trade

India's data sovereignty approach creates tensions with international trade obligations. The Regional Comprehensive Economic Partnership (RCEP) and bilateral investment treaties generally favor free data flows. India's withdrawal from RCEP negotiations partly reflected these data flow disagreements.

The 2025 withdrawal of equalization levies on digital advertising services, following trade pressure, illustrates the complex negotiation between sovereignty assertions and economic pragmatism (TechPolicy.Press, 2025). This suggests that India's data sovereignty framework remains subject to geopolitical and economic forces beyond purely legal considerations.

VI. THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: INTEGRATIVE FRAMEWORK

The (DPDPA 2023) represents India's comprehensive attempt to create an integrated data protection framework applicable to both DPIs and private sector data processing. This section analyzes key provisions and their implications for Aadhaar and UPI.

6.1. Scope and Applicability

The Act applies to processing of "digital personal data" within India and to offshore processing for offering goods/services to individuals in India (Digital Personal Data Protection Act, 2023), Section 2. This extraterritorial application extends India's regulatory reach globally, similar to GDPR.

Critically, the Act applies to both government and private entities, creating uniform standards across public and private sectors. However, Section 17 provides broad exemptions for government processing in the interest of sovereignty, security, public order, and friendly relations with foreign states. These exemptions have drawn criticism for potentially undermining the Act's protective scope.

6.2. Core Principles and Rights

The Act establishes several foundational principles:

- Consent-Based Processing: Requires "free, specific, informed, clear and unambiguous" consent for data processing, with explicit prohibition of forced or coercive consent (Section 6).
- Purpose Limitation:Data may be processed only for specified purposes, with new purposes requiring fresh consent (Section 4).
- Data Minimization: Collection must be limited to what is necessary for the specified purpose (Section 8).
- Storage Limitation: Data must be erased upon purpose completion or consent withdrawal (Section 8).

- Security Safeguards: Mandatory implementation of reasonable security measures (Section 8).
- Accountability: Data fiduciaries bear full responsibility for compliance, including for processors acting on their behalf (Section 8).

6.3. Data principals (individuals) receive several rights:

- Right to access collected data and processing purposes (Section 11)
- Right to correction and completion of data (Section 11)
- Right to erasure (with exceptions for legal obligations) (Section 11)
- Right to grievance redressal (Section 11)
- Right to nominate in case of death or incapacity (Section 11)

6.4. Application to DPIs

For Aadhaar and UPI, the DPDPA creates several implications:

Enhanced Consent Requirements: Both systems must ensure consent mechanisms meet the Act's standards. For Aadhaar, this reinforces the 2024 regulatory amendments requiring explicit, informed consent. For UPI, this mandates clearer data sharing disclosures.

Consent Managers: The provision for registered consent managers creates new intermediaries for managing consent across multiple platforms, potentially including UPI-integrated services.

Breach Notification: Both UIDAI and NPCI must notify the Data Protection Board of breaches "as soon as possible," creating new transparency obligations (Section 8).

Government Exemptions Challenge: Section 17's broad exemptions potentially undermine protections. If government entities operating Aadhaar invoke sovereignty or security exemptions, core protections (notice, consent) may not apply, creating a two-tier system.

6.5. Limitations and Critiques

Several limitations undermine the DPDPA's effectiveness:

Weak Enforcement Architecture: The Data Protection Board's powers, composition, and independence remain unclear pending rules notification. Without strong institutional backing, rights remain theoretical.

Broad Government Exemptions: Section 17 exemptions lack procedural safeguards or oversight mechanisms. Unlike GDPR's necessity and proportionality requirements for government processing, Indian framework grants wide discretion.

Absence of "Right to Be Forgotten": Unlike GDPR, the DPDPA provides only a right to erasure subject to extensive exceptions, limiting individual control.

Limited Data Portability: The Act does not establish robust data portability rights, hindering user mobility across platforms.

Penalty Uncertainty: Penalties up to ₹250 crores seem substantial, but effectiveness depends on enforcement, which remains untested.

VII. IDENTIFIED GAPS AND PERSISTENT CHALLENGES

Despite the sophisticated legal architecture, several critical gaps persist:

7.1. Consent in Contexts of Compulsion

The fundamental tension between voluntary consent and practical compulsion remains unresolved. When Aadhaar becomes necessary for welfare benefits or when UPI becomes the dominant payment modality, consent becomes illusory. The legal framework acknowledges this through Section 7 of the Aadhaar Act but fails to establish adequate compensatory safeguards.

Research documenting authentication failures leading to welfare denial highlights how technical glitches transform consent-based systems into exclusionary mechanisms (Privacy International, 2018). The legal framework lacks provisions addressing such technological failures' rights implications.

7.2. Accountability Deficits

Institutional Accountability: Neither UIDAI nor NPCI are subject to robust public accountability mechanisms. UIDAI lacks an independent oversight body, while NPCI's hybrid status creates ambiguities about transparency obligations.

Algorithmic Accountability: Both systems employ algorithmic decision-making (biometric matching, fraud detection), yet neither the Aadhaar Act nor UPI regulations establish algorithmic accountability standards. The absence of explainability requirements, bias auditing, or algorithmic impact assessments represents a significant gap.

Remedy Limitations: Existing grievance mechanisms lack independence and accessibility. Justice Chandrachud highlighted this in his dissent, noting the absence of effective remedies for rights violations (Justice K.S. Puttaswamy v. Union of India, 2018).

7.3. Data Sovereignty Implementation Challenges

Localization vs. Security: The assumption that data localization enhances security remains empirically unproven. India's data center infrastructure may lack security sophistication of global providers, potentially increasing rather than decreasing vulnerability.

Cross-Border Flow Uncertainty: The DPDPA's "restricted country" approach lacks clear standards for assessments. The absence of adequacy criteria (unlike GDPR's detailed framework) grants excessive executive discretion, creating legal uncertainty for businesses.

Sovereignty-Privacy Tension: Data sovereignty measures that concentrate data domestically may facilitate state surveillance, creating tension with privacy protection objectives. The legal framework does not adequately address this paradox.

7.4. Enforcement and Implementation Gaps

Delayed Rules: Despite DPDPA passage in 2023, rules notification remains pending, leaving critical provisions inoperative. This delay undermines legal certainty and rights realization.

Data Protection Board: The Board's non-operationalization means no enforcement authority exists. Without institutional infrastructure, even strong provisions remain paper tigers.

Capacity Constraints: Implementing consent, accountability, and sovereignty frameworks requires significant technical and administrative capacity. Whether government and private entities possess such capacity remains questionable.

7.5. Exclusion and Marginalization

Digital Divide: Both Aadhaar and UPI assume digital literacy and access. Marginalized populations lacking these resources face exclusion, yet the legal framework provides inadequate accommodations.

Biometric Failure Impacts: Authentication failure rates, particularly for manual laborers with worn fingerprints or elderly citizens with degraded biometrics, create systematic exclusion. The legal framework lacks provisions for alternative authentication or failure liability.

Language and Accessibility: Despite DPDPA's requirement for notices in scheduled languages, implementation remains inconsistent, creating informational barriers for non-English speakers.

VIII. RECOMMENDATIONS AND REFORM DIRECTIONS

8.1. Strengthening Consent Mechanisms

Contextual Consent Standards: Develop differentiated consent standards recognizing power asymmetries. For essential services, implement "compensatory safeguards" including enhanced transparency, accountability, and remedy provisions.

Consent Audit Requirements: Mandate periodic third-party audits of consent mechanisms, particularly for DPIs, evaluating whether consent is genuinely informed and voluntary.

Alternative Authentication: Strengthen legal requirements for alternative authentication methods when biometric systems fail, ensuring technology does not become a barrier to rights realization.

8.2. Enhancing Accountability Structures

Independent Oversight: Establish an independent Aadhaar Oversight Authority separate from UIDAI, modeled on information commissions or ombudsman institutions, with powers to investigate complaints and recommend sanctions.

NPCI Accountability Framework: Clarify NPCI's legal status and establish explicit transparency obligations, including public reporting requirements, stakeholder consultation procedures, and judicial review provisions.

Algorithmic Accountability Standards: Develop specific regulations governing algorithmic systems in DPIs, including requirements for bias testing, explainability, human oversight, and impact assessments.

Effective Remedy Mechanisms: Strengthen grievance redress through dedicated tribunals with expertise in technology and rights, accessible through multiple channels including mobile apps and citizen service centers.

8.3. Operationalizing Data Sovereignty

Clear Adequacy Standards: Develop transparent, rule-bound standards for assessing cross-border transfer destinations, considering rule of law, independent oversight, and reciprocity principles, similar to GDPR's adequacy framework.

Security Standards: Rather than assuming localization ensures security, establish explicit security standards for data storage and processing regardless of location, with mandatory compliance verification.

Surveillance Safeguards: Enact comprehensive surveillance reform limiting government access to DPI data to legitimate, necessary purposes, subject to judicial oversight and proportionality requirements.

8.4. Institutional and Enforcement Reforms

Expedite Rules Notification: Prioritize notification of DPDPA rules and operationalization of the Data Protection Board to give effect to statutory protections.

Capacity Building: Invest in technical and administrative capacity development for government agencies, judiciary, and civil society to effectively implement and monitor the complex regulatory framework.

Transparency Requirements: Mandate comprehensive transparency reporting by UIDAI, NPCI, and other DPI operators, including transaction volumes, authentication failure rates, breach incidents, and grievance statistics.

8.5. Inclusive Design and Implementation

Accessibility Standards: Develop comprehensive accessibility standards ensuring DPIs are usable by persons with disabilities, elderly citizens, and populations with limited digital literacy.

Multi-Modal Authentication: Move beyond biometric-only systems to incorporate multiple authentication modalities, including knowledge-based and possession-based factors.

Offline Capabilities: Develop offline authentication capabilities for contexts lacking network connectivity, ensuring technology does not exclude rural and remote populations.

IX. CONCLUSION

India's legal architecture for Digital Public Infrastructures represents an ambitious attempt to harness technology for governance transformation while protecting fundamental rights. Through the Aadhaar Act, NPCI regulations, and the (DPDPA 2023), India has constructed a multilayered framework addressing consent, accountability, and data sovereignty.

The framework demonstrates several strengths: constitutional grounding through the Puttaswamy judgments, comprehensive consent provisions, evolving accountability mechanisms, and nuanced approaches to data sovereignty that balance nationalism with pragmatism. The Supreme Court's 2018 Aadhaar judgment particularly stands out for its careful balancing analysis, striking unconstitutional provisions while preserving the system's core.

However, persistent gaps undermine the framework's effectiveness. Consent mechanisms struggle with inherent power asymmetries when dealing with essential services. Accountability structures lack institutional independence and enforcement capacity. Data sovereignty approaches risk creating security paradoxes while potentially facilitating surveillance. Most critically, the delayed implementation of the DPDPA leaves rights unrealized and protections theoretical.

The tension between technological efficiency and rights protection remains unresolved. India's DPI model privileges scale, speed, and inclusion, sometimes at the expense of consent validity, accountability robustness, and sovereignty protection. Whether this trade-off is justified depends on normative commitments about the relationship between state, technology, and individual autonomy.

As India's DPI model gains global attention, the lessons from its legal architecture become internationally significant. Other nations considering similar systems must learn both from India's innovations—such as consent managers and hybrid public-private models—and from its challenges—including accountability deficits and implementation gaps.

The legal architecture's ultimate success will depend not merely on statutory texts but on institutional capacity, political will, and sustained civil society vigilance. Strong laws remain insufficient without strong institutions to implement them, dedicated resources to operationalize them, and engaged citizenry to demand accountability.

India stands at a critical juncture. The framework elements are in place, but realization requires action: operationalizing the Data Protection Board, notifying pending rules, establishing independent oversight, developing algorithmic accountability standards, and ensuring that technological innovation serves rather than subverts constitutional commitments to dignity, equality, and liberty.

The coming years will determine whether India's legal architecture for DPIs becomes a model for democratic digital governance or a cautionary tale about technology outpacing law, scale overwhelming rights, and efficiency eclipsing accountability. The stakes extend beyond India, as the answer will influence how democracies worldwide navigate the fundamental challenge of our era: harnessing digital transformation while preserving human dignity and freedom.

REFERENCES

Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (India).

Bovens, M. (2007). Analysing and assessing accountability: A conceptual framework. *European Law Journal, 13*(4), 447–468. https://doi.org/10.1111/j.1468-0386.2007.00378.x

Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India). Retrieved from https://www.meity.gov.in/content/digital-personal-data-protection-act-2023

Hariharan, V., & Natarajan, S. (2024). Digital sovereignty and payments: A case study of the National Payments Corporation of India. In M. Jiang & L. Belli (Eds.), *Digital sovereignty in the BRICS countries: How the Global South and emerging power alliances are reshaping digital governance*. Cambridge University Press.

Indusface. (2025, August 13). *NPCI UPI API security (OC-215) compliance.* https://www.indusface.com/blog/npci-upi-api-security-guidelines/

Jiang, M. (2024). Models of state digital sovereignty from the Global South: Diverging experiences from China, India and South Africa. *Policy & Internet, 16*(4), 427–451. https://doi.org/10.1002/poi3.427

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (Supreme Court of India).

Justice K.S. Puttaswamy (Retd.) v. Union of India, Writ Petition (Civil) No. 494 of 2012 (Supreme Court of India, 2018). Retrieved from https://uidai.gov.in/images/news/Judgement_26-Sep-2018.pdf

Ministry of Electronics and Information Technology. (2023). *Digital Personal Data Protection Act, 2023.* Government of India. https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

National Payments Corporation of India. (2024). *UPI product statistics.* Retrieved from https://www.npci.org.in/what-we-do/upi/product-statistics

National Payments Corporation of India. (2025). *Unified Payments Interface circulars.* Retrieved from https://www.npci.org.in/what-we-do/upi/circular

NPCI. (2025, March 31). *NPCI brings new UPI guidelines in effect from April 1, 2025. Elets BFSI.* https://bfsi.eletsonline.com/npci-brings-new-upi-guidelines-in-effect-from-april-1-2025/
NPCI. (2025, August 1). *NPCI tightens UPI API rules to boost resilience, fraud controls. IBS Intelligence.* https://ibsintelligence.com/ibsi-news/npci-tightens-upi-api-rules-to-boost-resilience-fraud-controls/
Payment and Settlement Systems Act, 2007 (India).
Privacy International. (2018, September 26). *Initial analysis of Indian Supreme Court decision on Aadhaar*. Retrieved from https://privacyinternational.org/long-read/2299/initial-analysis-indian-supreme-court-decision-aadhaar
Rajmohan, K. (2025, January 23). *Data localization: India's tryst with data sovereignty. TechPolicy.Press.* https://www.techpolicy.press/data-localization-indias-tryst-with-data-sovereignty/
Reserve Bank of India. (2018, April 6). *Storage of payment system data (Circular No. RBI/2017-18/153).* Mumbai: Reserve Bank of India.
Sieker, F., & Lloyd, T. (2024). *From India Stack to EuroStack: Reconciling approaches to sovereign digital infrastructures (ECDPM Discussion Paper No. 384).* European Centre for Development Policy Management.
Solove, D. J. (2013). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review, 126*(7), 1880–1903.
Spice Route Legal. (2025, April 10). *Comply with DPDPA and Aadhaar as one. Law.Asia.* https://law.asia/aadhaar-dpdpa-compliance/
Stratink Consulting. (2025, August 1). *How Indian tech policy is pushing for digital sovereignty.*
TechPolicy.Press. (2025). *India's search for digital sovereignty.* https://www.techpolicy.press/indias-search-for-digital-sovereignty/
Unique Identification Authority of India. (2024). *Aadhaar dashboard* [Data set]. Retrieved from https://uidai.gov.in/aadhaar_dashboard/
Unique Identification Authority of India. (2024). *The Aadhaar (Enrolment and Update) Amendment Regulations, 2024.* Retrieved from https://uidai.gov.in/en/about-uidai/legal-framework/regulations/
Verfassungsblog. (2025, March 12). *Cross-border data flows and India's digital sovereignty.* https://verfassungsblog.de/cross-border-data-flows-and-indias-digital-sovereignty/