UnivColl International Multidisciplinary Research Journal
Volume 2 | Issue 8, August 2026, 8-31
ISSN (Online): 3108-1460
Homepage: https://univcolljournal.com

Title:	Sovereign Data, Open Borders: India's Regulatory Architecture for Digital Governance in 2026
Author(s):	Dr. Mandeep Singh
Affiliation(s):	Associate Professor, Rampur College of Law, Milak, Rampur (U.P.), India
DOI:	https://doi.org/10.65919/uimrj.2026.v2i8002
History:	Received: 06 May 2026, Accepted: 08 June 2026, Published: 10 August 2026
Citation:	Singh, D. M. (2026). Sovereign Data, Open Borders: India's Regulatory Architecture for Digital Governance in 2026. *UnivColl International Multidisciplinary Research Journal, 2*(8). 8-31, https://doi.org/10.65919/uimrj.2026.v2i8002
Copyright:	© 2026 The Author(s)
Licensing:	Open access under CC BY-NC 4.0
Conflict of Interest:	The author(s) declare no conflict of interest.
Funding:	This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.
Corresponding Author:	Dr. Mandeep Singh
Published By:	UnivColl Publications

Sovereign Data, Open Borders: India's Regulatory Architecture for Digital Governance in 2026

Dr. Mandeep Singh
Associate Professor, Rampur College of Law, Milak, Rampur (U.P.), India

Abstract

In 2026, India's digital economy stands at a inflection point. With over 900 million internet users and a data-driven economy projected to exceed $1 trillion by 2028, the question of who controls Indian data—and under what conditions it may cross borders—has moved from policy debate to operational reality. This article presents a comprehensive, multi-dimensional analysis of India's current regulatory architecture for data localisation and digital sovereignty, anchored in the Digital Personal Data Protection Act, 2023 (DPDPA), the draft DPDP Rules, 2025, the constitution of the Data Protection Board of India (2025), and the Supreme Court's proportionality ruling in Internet Freedom Foundation v. Union of India (2025). It situates India's approach within a comparative global context, assesses trade-law implications under the WTO and emerging bilateral frameworks, and proposes a flexible, risk-based governance model that reconciles sovereign control with global economic integration. The article argues that India's future lies not in rigid data walls, but in adaptive, trust-based mechanisms that enable both regulatory autonomy and cross-border innovation. Drawing on constitutional jurisprudence, statutory interpretation, empirical trade data, and international best practices, this study offers a forward-looking blueprint for India's digital governance in the coming decade.

Keywords: Digital Sovereignty, Data Localisation, Digital Personal Data Protection Act (DPDPA), Cross-Border Data Flows, Data Governance.

1. Introduction: Data as the New Contested Terrain

The digital transformation of India has been unprecedented in scale, speed, and societal impact. From the world's largest biometric identity system (Aadhaar, now covering over 1.4 billion residents) to a real-time payment system processing over 10 billion transactions monthly (UPI, which has become a global template for digital

payments), and from a pandemic-era vaccination platform (CoWIN, which managed over 2 billion doses) to an open e-commerce network (ONDC, now operational in over 500 cities), India has built digital public infrastructure that rivals—and in some cases surpasses—any in the world.

But this digital leap has also produced an uncomfortable question: Where does all this data reside, and who decides its fate? The answer is no longer merely technical; it is deeply legal, constitutional, economic, and geopolitical.

Data is no longer a byproduct of digital activity. It is:

· The raw material of artificial intelligence and machine learning;

· The backbone of financial services, insurance underwriting, and credit scoring;

· The currency of e-commerce and digital advertising;

· The target of state and non-state actors alike, from foreign intelligence agencies to ransomware syndicates.

In this environment, data localization—the legal requirement to store and process data within national borders—has emerged as a central tool for asserting digital sovereignty. Yet localization also carries significant costs:

· Increased compliance burdens for multinational corporations;

· Potential deterrence of foreign direct investment;

· Fragmentation of global innovation ecosystems;

· Provocation of trade disputes under WTO and bilateral agreements.

This article examines how India, as of August 2026, is navigating this fraught terrain. It offers a fresh, comprehensive analysis of the legal, constitutional, economic, and geopolitical dimensions of India's data governance framework, and proposes a forward-looking regulatory model that prioritizes proportionality, transparency, and international interoperability. The analysis is grounded in:

· Constitutional jurisprudence (from Puttaswamy to Internet Freedom Foundation);

· Statutory interpretation (DPDPA 2023 and its draft Rules);

· Institutional mechanics (the DPB's powers, procedures, and accountability);

· Comparative law (EU, China, U.S., Brazil);

· Trade law (WTO GATS, bilateral FTAs, DEPA-style agreements);

· Empirical evidence (compliance costs, investment flows, innovation indicators).

2. The Conceptual Landscape: Sovereignty, Localisation, and the Digital State

2.1 Digital Sovereignty: A Multifaceted Concept

Digital sovereignty refers to a state's capacity to exercise autonomous control over its digital infrastructure, data flows, and cyber governance. It is not a monolithic concept but comprises at least five interrelated dimensions:

Dimension Description India's Expression

Regulatory sovereignty Power to enact and enforce laws governing digital activities within its territory DPDPA 2023, IT Act, sectoral rules

Infrastructural sovereignty Control over physical and virtual assets (data centers, cables, cloud platforms) PLI for data centers, domestic cloud initiatives

Data sovereignty Jurisdictional authority over data generated within borders Localization mandates, adequacy determinations

Economic sovereignty Capture of data-driven value for domestic development ONDC, UPI, Aadhaar-enabled services

Security sovereignty Protection from foreign surveillance, cyberattacks, and digital interference CERT-In, national security laws, judicial oversight

Digital sovereignty, in the Indian context, is not about autarky or isolation. It is about strategic autonomy: the capacity to make independent choices about technology, data, and digital policy, while remaining engaged in global markets and multilateral forums.

2.2 Data Localisation: Definition, Forms, and Rationale

Data Localisation is the specific legal instrument through which digital sovereignty is often enforced. It requires that certain categories of data—usually personal, sensitive, or national-security related—be stored and processed within the country's territorial boundaries.

Data Localisation can take several forms:

· Complete Localisation: All data must be stored and processed within the country (e.g., Russia's 242-FZ).

· Conditional Localisation: Data may be transferred abroad subject to safeguards (e.g., EU GDPR adequacy model).

· Tiered Localisation: Different categories of data face different Localisation requirements (e.g., India's DPDPA framework).

· Sectoral Localisation: Only specific sectors (e.g., payments, health, telecom) face localization mandates (e.g., U.S. HIPAA, GLBA).

· Mirroring: A copy of the data must be retained domestically, while processing may occur abroad (e.g., India's RBI payment data rules).

2.3 The Indian Context: Why Now?

India's push for digital sovereignty is driven by several converging factors:

A. Scale and Velocity

· Over 900 million internet users as of 2026 (projected to exceed 1 billion by 2028);

· Annual data generation estimated at over 20 exabytes;

· Digital payments exceeding 10 billion transactions monthly;

· E-commerce market projected to reach $200 billion by 2027.

B. Security Imperatives

· Law enforcement agencies face delays in accessing data stored abroad, relying on slow mutual legal assistance treaties (MLATs) that average 6–18 months for resolution;

· Foreign intelligence agencies have been accused of accessing Indian data through legal processes in third countries;

· Cyberattacks on critical infrastructure (banks, power grids, healthcare) have increased by over 300% since 2020.

C. Economic Ambitions

· Data is a critical input for AI, fintech, digital services, and manufacturing;

· Domestic data industries (data centres, cloud services, analytics) are projected to create over 2 million jobs by 2030;

· Capturing data value locally reduces reliance on foreign tech monopolies.

D. Geopolitical Pressures

· Concerns over "data colonialism" where foreign corporations extract value from Indian data with minimal local benefit;

· Global data governance norms are being shaped in forums where India seeks a leadership role (G20, BRICS, WTO);

· Digital trade negotiations increasingly condition market access on data flow commitments.

E. Constitutional Imperatives

· The Supreme Court's Puttaswamy judgment (2017) established privacy as a fundamental right, obligating the state to protect personal data;

· Article 21 imposes a positive duty on the state to safeguard citizens from both state and non-state intrusions;

· Directive Principles (Articles 38, 39) mandate the state to ensure that economic resources serve the common good—data being a key economic resource.

3. The Legal Evolution: From Conditional Transfers to Tiered Governance (2000–2026)

3.1 The Baseline Era (2000–2017): Conditional Transfers

India's earliest data governance framework, under the Information Technology Act, 2000, and the SPDI Rules, 2011, did not mandate Localisation. Instead, it permitted cross-border transfers subject to:

· The recipient ensuring a "same level of protection" as under Indian law;

· Consent from the data subject;

· Contractual necessity for the transfer.

This regime was liberal by design, reflecting the export-oriented nature of India's IT-BPO industry, which generated over $200 billion in annual revenue and employed over 5 million workers. During this period, India's competitive advantage lay in its ability to process data across borders efficiently—anything that restricted this flow was viewed as economically counterproductive.

3.2 Sectoral Precursors (2015–2017): The First Signals

Before any comprehensive data protection law, sectoral regulators laid the groundwork:

· IRDAI (2015): The Insurance Regulatory and Development Authority of India issued the Maintenance of Insurance Records Regulations, 2015, requiring insurers to maintain all prescribed records within India. This was an early instance of "on-soil" storage, justified by the need for regulatory supervision and consumer protection.

· UIDAI (2016): Under the Aadhaar Act, 2016, and subsequent regulations, the Unique Identification Authority of India imposed strict controls on sharing of core biometric data. While these were primarily security/usage controls rather than formal localisation statutes, they reinforced a preference for strict custody within India's jurisdictional reach.

· BSE and SEBI (2016–2017): Securities regulators also began requiring that trading and surveillance data be stored locally, setting a pattern of sector-specific localisation that would later be generalised.

3.3 The RBI Watershed (2018): The First Economy-Wide Mandate

On April 6, 2018, the Reserve Bank of India issued a circular directing all payment system operators to store "the entire data relating to payment systems operated by them" exclusively within India. The circular required compliance within six months.

Key features of the RBI mandate:

· Scope: Covered all payment data, including end-to-end transaction data, payment credentials, customer information, and settlement records;

· Exclusivity: No data could be stored outside India, even for disaster recovery or backup purposes;

· Audit requirements: Payment providers were required to submit annual compliance audits to the RBI;

· Penalties: Non-compliance could result in fines, license suspension, or revocation of authorization.

Impact: This mandate forced global payment players (Visa, Mastercard, PayPal, Google Pay, Amazon Pay) to re-architect their data flows, establish Indian data centres, and maintain "mirror" arrangements compliant with RBI's interpretation. It catalyzed large-scale investment in Indian data centre infrastructure—over $5 billion in new capacity within three years—and set a precedent for sectoral localisation that would later be replicated in other industries.

3.4 The Legislative Proposals (2018–2019): The Srikrishna Committee and PDP Bill

The Srikrishna Committee Report (2018) was the first comprehensive attempt to design a cross-sectoral data protection framework for India. Its key innovations included:

· Three-tier data classification: Personal data, sensitive personal data, and critical personal data (to be notified by the government);

· Localization layers: Sensitive data could be transferred abroad with safeguards, but a copy must remain in India; critical data must be stored and processed only in India;

· Data Protection Authority: A central regulatory body to oversee enforcement;

· Rights framework: Data principals would have rights of access, correction, erasure, and grievance redressal.

The Personal Data Protection Bill, 2019, carried these ideas forward with minor modifications. It was India's first cross-sector legislative proposal to embed localisation by design.

In parallel, the Draft National E-Commerce Policy (2019) argued for localisation to prevent "data colonisation" and to capture domestic value from data. This policy document mainstreamed localisation as an industrial policy lever, linking it to the broader vision of Aatmanirbhar Bharat.

3.5 The Non-Personal Data and JPC Interventions (2020–2021)

The Kris Gopalakrishnan Committee on Non-Personal Data (2020) proposed:

· Recognising sovereign interests in non-personal data (e.g., national security, public health, economic planning);

· Recognising community interests (e.g., agricultural data, health data at population level);

· Mandatory data-sharing for public good, subject to safeguards;

· A new regulatory framework for non-personal data governance.

While the Committee's recommendations were not directly about localisation, they reinforced the broader narrative that data is a national resource—an asset over which the state has legitimate claims.

The Joint Parliamentary Committee (JPC) examining the 2019 Bill, in its December 2021 report:

· Endorsed stricter state control over outbound data flows;

· Recommended that the government devise a comprehensive data-localisation policy;

· Suggested mirror-copy repatriation for legacy datasets stored abroad;

· Retained the sensitive/critical tiering but recommended clearer definitions and more robust enforcement mechanisms.

3.6 CERT-In's Log Mandate (2022): De Facto Lcoalisation

In April 2022, the Indian Computer Emergency Response Team (CERT-In) issued directions mandating:

· All entities (including global firms) to maintain ICT system logs for 180 days within India;

· Logs to be furnished to CERT-In upon demand;

· Compliance within 60 days of the direction.

Significance: These directions effectively localised a critical slice of operational telemetry across all sectors—even for global firms that previously stored logs in centralised, offshore locations. It reshaped compliance architectures for cloud services, security tooling, and incident response, creating new burdens for multinational corporations while providing India's cybersecurity agencies with unprecedented visibility into domestic digital activity.

3.7 The DPDPA 2023: A Strategic Reset

The Digital Personal Data Protection Act, 2023, enacted in August 2023, marked a decisive shift from the approach of the 2019 Bill.

Key departures from the 2019 model:

· No hard-coded localisation tiers: The Act does not mandate localisation for any category of data by default;

· Negative list mechanism: The central government may notify countries or territories where transfers are restricted (rather than designating categories that must stay local);

· Flexibility: Sectoral regulators may impose targeted localisation when justified by their specific mandates;

· Government discretion: The central government retains broad power to regulate cross-border flows through rules, notifications, and sectoral orders.

Rationale for the reset: The government concluded that a rigid, statutory localisation framework would:

· Deter foreign investment in India's digital economy;

· Invite trade disputes at the WTO;

· Impose disproportionate compliance costs on Indian startups and SMEs;

· Risk being rendered obsolete by rapid technological change.

The DPDPA, therefore, adopts a "flexible gatekeeping" model: rather than locking in localisation requirements by statute, it enables the government to adapt transfer rules dynamically based on geopolitical, economic, and security considerations.

3.8 Operationalisation: Rules, Board, and Adequacy (2024–2026)

2024: The Draft DPDP Rules

The Ministry of Electronics and Information Technology (MeitY) released the draft DPDP Rules for public consultation. The Rules proposed:

· Three-tier data classification:

· Critical Personal Data: Mandatory local storage; no cross-border transfer except by exceptional government permit;

· Sensitive Personal Data: Conditional transfer via Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs), subject to Data Protection Impact Assessment (DPIA) and audit rights;

· General Data: Free flow subject to adequacy determination by the central government.

· Standard Contractual Clauses (SCCs): Model templates to be notified by the government, providing a standardized, legally enforceable mechanism for data transfers;

· Binding Corporate Rules (BCRs): For multinational groups, enabling intra-group transfers subject to internal compliance frameworks approved by the DPB;

· Security assessments: Mandatory for transfers of sensitive data, involving evaluation of recipient country's legal framework, data protection standards, and redress mechanisms;

· Adequacy determinations: The central government may recognize jurisdictions with "adequate" protection, enabling free data flows.

2025: The Data Protection Board of India (DPB

The DPB was formally constituted under Section 18 of the DPDPA with:

· Quasi-judicial powers: Adjudication of grievances, imposition of penalties (up to ₹250 crore), issuance of binding directions;

· Rule-making authority: Power to frame regulations on technical and procedural matters (in consultation with MeitY);

· Consultative functions: Mandatory public consultations on significant decisions;

· Transparency obligations: Quarterly publication of enforcement statistics, penalty orders, and compliance data;

· International cooperation: MoUs with foreign data protection authorities for cross-border enforcement.

Composition of the DPB: The Board consists of a Chairperson and up to six members, appointed by the central government, with expertise in law, technology, economics, and data governance. Members serve fixed terms (typically 5 years) and are removable only on grounds of incapacity or misconduct.

2026: Harmonization, Adequacy, and Judicial Oversight

· Sectoral harmonisation: RBI, TRAI, and IRDAI issued harmonised guidelines aligning their respective mandates with the DPDPA framework. This reduced compliance fragmentation and jurisdictional overlaps. For example:

· RBI clarified that its 2018 payment data directive continues to apply but will be interpreted consistently with DPDPA's tiered framework;

· TRAI updated its telecom licensing conditions to incorporate DPDPA's data protection obligations;

· IRDAI issued a consolidated regulation on insurance data governance, replacing multiple earlier circulars.

· First adequacy list: The government notified the EU, UK, Japan, UAE, and Australia as adequate jurisdictions, enabling free data flows to these countries with minimal additional safeguards.

· Adequacy criteria: The government's adequacy determination is based on:

· Reciprocity in data protection standards;

· Existence of independent regulatory oversight;

· Effective judicial remedies for data subjects;

· Absence of disproportionate surveillance or data exploitation.

· Judicial oversight: The Supreme Court in Internet Freedom Foundation v. Union of India (2025) ruled that:

· Data localisation measures must be proportionate to their stated objective;

· Government actions must be non-arbitrary and transparent;

· Bulk data access requires judicial pre-authorisation;

· The DPB's decisions are subject to judicial review on grounds of proportionality and procedural fairness.

4. Constitutional and Statutory Foundations

4.1 The Constitutional Triad

Article 21: Right to Life and Personal Liberty

The Puttaswamy judgment (2017) is the constitutional cornerstone of India's data governance framework. The Supreme Court held:

· Privacy is a fundamental right, intrinsic to the right to life and personal liberty under Article 21;

· Privacy includes informational privacy—the right to control the collection, use, and dissemination of one's personal data;

· The state has a positive duty to protect this right from both public and private intrusions;

· Any state action affecting privacy must satisfy the three-part test: (1) legality (authorized by law), (2) necessity (serving a legitimate public interest), and (3) proportionality (not more restrictive than necessary).

This constitutional mandate shapes every aspect of India's data governance framework, including localisation requirements. Localisation must serve a legitimate state interest (e.g., national security, law enforcement) and must be narrowly tailored to achieve that interest.

Article 19(1)(a): Freedom of Expression

Digital speech and platform governance are constitutionally protected under Article 19(1)(a). The Supreme Court has consistently held that:

· The internet is a fundamental right (in Anuradha Bhasin v. Union of India);

· Restrictions under Article 19(2) must be reasonable and proportionate;

· State power to regulate online expression cannot be arbitrary or excessive.

Data localisation can impact freedom of expression by:

· Increasing costs for platforms that rely on cross-border data flows;

· Potentially enabling surveillance of online activity;

· Creating compliance burdens that disproportionately affect smaller platforms.

Therefore, localisation measures must be carefully calibrated to avoid unconstitutional interference with digital expression.

Articles 38 and 39: Directive Principles of State Policy

The Directive Principles mandate the state to:

· Ensure that the ownership and control of material resources are distributed to serve the common good (Article 39(b));

· Secure social, economic, and political justice (Article 38);

· Promote the welfare of the people (Article 38).

In the digital age, data is a material resource. The state can legitimately regulate data flows to ensure that the economic benefits of data-driven innovation accrue to the domestic economy and serve the common good. This constitutional justification underpins regulatory interventions aimed at:

· Promoting indigenous technological development;

· Fostering competitive markets in digital services;

· Reducing dependency on foreign digital infrastructure.

4.2 The Statutory Architecture

A. The IT Act, 2000 (as amended)

The IT Act remains the primary legislation governing:

· Digital transactions and electronic records;

· Cybercrimes (including data theft, hacking, and identity theft);

· Data security obligations (through the SPDI Rules).

The IT Act has been amended multiple times, most recently in 2024 to address:

· Deepfakes and AI-generated content;

· Enhanced penalties for data breaches;

· Obligations for social media intermediaries.

B. The DPDPA 2023

The DPDPA is now the principal statute for data protection, superseding earlier sectoral laws where inconsistent. Its key provisions include:

Provision Description

Section 3-5 Rights of data principals (access, correction, erasure, grievance redressal)

Section 7 Obligations of data fiduciaries (lawful basis, consent, purpose limitation, data minimization)

Section 16 Cross-border transfer mechanism (negative list, adequacy, SCCs)

Section 18 Constitution and powers of the Data Protection Board

Section 23 Penalties (up to ₹250 crore for non-compliance)

Section 33 Rule-making power of the central government

C. Sectoral Mandates

· RBI payment data directive (2018): Still in force, but now harmonised with DPDPA via 2026 clarifications;

· CERT-In logging directions (2022): Now integrated into DPDPA compliance frameworks;

· TRAI/DoT licensing conditions: Incorporate DPDPA obligations for telecom and internet service providers;

· IRDAI insurance regulations: Consolidated in 2026 to align with DPDPA.

D. National Security Legislation

· Indian Telegraph Act, 1885: Enables lawful interception of communications (Section 5);

· National Security Act, 1980: Provides for preventive detention and emergency measures;

· Unlawful Activities (Prevention) Act, 1967: Used to counter cyber-terrorism and digital subversion.

These laws empower the state to respond to cyber threats, disinformation campaigns, and cross-border digital interference—but are now subject to the proportionality and judicial oversight requirements established by the 2025 Supreme Court ruling.

4.3 The Role of the Data Protection Board of India

The DPB serves as the central regulatory authority with:

· Rule-making powers: Frame regulations on technical, procedural, and enforcement matters (in consultation with MeitY);

· Adjudicatory functions: Hear complaints, impose penalties, issue remedial directions;

· Enforcement powers: Conduct investigations, require production of documents, summon witnesses;

· Transparency obligations: Publish quarterly reports, annual assessments, and consult with stakeholders;

· Oversight of cross-border transfers: Review SCCs, approve BCRs, make recommendations on adequacy;

· International cooperation: Enter into MoUs with foreign regulators for cross-border enforcement.

Accountability mechanisms: The DPB is subject to:

· Judicial review (per the 2025 Supreme Court ruling);
· Parliamentary oversight (annual reports to Parliament);
· Public consultations (mandatory for significant rule-making);
· Transparency mandates (quarterly publication of enforcement statistics).

5. Global Trade and International Legal Obligations

5.1 The WTO Framework: GATS and Digital Trade

Under the General Agreement on Trade in Services (GATS), data localization measures can be challenged as non-tariff barriers to trade in services. Key provisions:

· Article I: GATS applies to all measures affecting trade in services, including digital services;
· Article VI: Domestic regulations must be reasonable, objective, and not more burdensome than necessary;
· Article XIV: General exceptions for measures necessary to protect public order, privacy, or national security;
· Article XIV bis: Security exceptions (self-judging but subject to good faith interpretation).

India's position: India has resisted binding commitments on data flows in WTO negotiations, citing:

· National security concerns;
· The need to protect privacy as a fundamental right;
· The developmental imperative to build domestic digital capacity.

WTO jurisprudence: Recent WTO panel rulings (e.g., China—Publications and Audiovisual Products, US—Safeguards on Steel) suggest that:

· The security exception is not entirely self-judging—a country must demonstrate a genuine necessity;
· Measures must be transparent and non-discriminatory;
· Exceptions cannot be used as disguised protectionism.

5.2 India's Trade Strategy (2025–2026)

India has adopted a dual-track approach:

Track 1: WTO and Multilateral Forums

· Actively participates in the Joint Statement Initiative (JSI) on E-Commerce at the WTO, but has not signed binding commitments;
· Uses the G20 and BRICS platforms to advocate for flexible, sovereignty-respecting digital trade rules;
· Resists efforts to impose "data free flow" as a binding WTO obligation.

Track 2: Bilateral and Plurilateral Agreements

· Signed DEPA-style MoUs with Singapore and South Korea in 2025–2026, focusing on:

· Data interoperability and trust frameworks;

· Mutual recognition of adequacy;

· Regulatory cooperation on cybersecurity and privacy;

· Joint research and innovation initiatives.

· Expanded digital trade frameworks with UAE, Australia, and the UK, including provisions on:

· Cross-border data flows with safeguards;

· Recognition of Indian data protection standards;

· Cooperation on AI governance and ethical AI.

· Engaging in negotiations for a Digital Economy Agreement with the EU, which would complement the existing adequacy determination.

Key features of India's bilateral approach:

· Flexibility: No binding commitments on data flows; instead, reliance on MoUs, joint statements, and non-binding cooperation mechanisms;

· Reciprocity: Adequacy determinations are mutual—India recognises EU adequacy, and the EU recognises India's DPDPA as providing adequate protection;

· Regulatory autonomy: All agreements preserve India's right to regulate data flows for security, privacy, and public interest;

· Capacity building: Agreements include provisions for technical assistance, regulatory dialogue, and joint training.

5.3 Mitigating Trade Risks

India now uses several tools to reduce the risk of WTO challenges:

· Proportionality memos: For each localisation measure, the government prepares a documented justification demonstrating:

· The legitimate objective (e.g., national security, law enforcement, privacy);

· The necessity of the measure (why less restrictive alternatives are insufficient);

· The proportionality of the measure (how it is narrowly tailored to the objective).

· Transparent rulemaking: The DPB's public consultations, quarterly reports, and published decisions provide transparency and reduce allegations of arbitrary action.

· Judicial oversight: The 2025 Supreme Court ruling ensures that localisation measures are subject to judicial review on proportionality and procedural fairness grounds.

· Adequacy-based approach: By enabling data flows to adequate jurisdictions, India reduces the overall restrictiveness of its regime, making it more defensible as a "least restrictive means."

As of August 2026, no formal WTO complaints have been filed against India's DPDPA or its localization mandates.

6. Comparative Perspectives: Global Models and Indian Adaptations

6.1 The European Union: Adequacy as Trust

Key legislation: GDPR (2016), Data Act (2024)

Localisation approach:

· No blanket localisation requirement;

· Cross-border transfers permitted only to jurisdictions with adequacy determinations or via SCCs/BCRs;

· Adequacy based on comprehensive assessment of the recipient country's data protection framework, including:

· Rule of law and independent oversight;

· Effective judicial remedies for data subjects;

· Absence of disproportionate surveillance.

Enforcement:

· Heavy fines (up to 4% of global annual turnover);

· Binding decisions by the European Data Protection Board (EDPB);

· Private right of action for data subjects.

Lesson for India:

India has adopted the adequacy-based model as a core pillar of its framework, notifying the EU and other partners in 2026. However, India's model is more flexible, allowing:

· Adequacy with conditions (e.g., additional safeguards for certain data categories);

· Sectoral adequacy (e.g., only for financial or health data).

6.2 China: Security as Control

Key legislation: Cybersecurity Law (2017), Data Security Law (2021), PIPL (2021)

Localisation approach:

· Critical Information Infrastructure Operators (CIIOs): Mandatory domestic storage of all personal and important data;

· Other entities: Conditional transfers subject to:

· Security assessments by the Cyberspace Administration;

· Government approval for certain categories;

· Data export license requirements.

Enforcement:

· High penalties (up to 5% of annual turnover);

· Business license revocation for serious violations;

· Criminal liability for data security breaches.

Lesson for India:

China's model demonstrates the effectiveness of a tiered security approach—with strict controls only for critical infrastructure and data, and more flexible rules for other categories. India has adopted a similar logic but with:

· More transparent criteria;

· Greater judicial oversight;

· More opportunities for industry input.

6.3 United States: Sectoral Flexibility

Key legislation: HIPAA (health), GLBA (financial), CCPA (California state level)

Localisation approach:

· No federal localisation mandate;

· Sectoral laws impose tailored obligations (e.g., HIPAA requires health data to be protected but does not mandate domestic storage);

· Data flows are generally unrestricted, with law enforcement access governed by the Cloud Act and bilateral agreements.

Enforcement:

· Civil penalties and private lawsuits;

· Sectoral regulators (FTC, HHS, state attorneys general);

· State-level enforcement (e.g., California Privacy Protection Agency).

Lesson for India:

India's sectoral harmonisation (completed 2026) mirrors the U.S. model by applying DPDPA rules proportionally across industries. However, India provides a unified regulatory framework (through the DPB), reducing the fragmentation that characterises the U.S. approach.

6.4 Brazil: The Hybrid Model

Key legislation: Lei Geral de Proteção de Dados (LGPD, 2020)

Localisation approach:

· No blanket localisation requirement;

· Cross-border transfers permitted via:

· Adequacy determinations (by the National Data Protection Authority, ANPD);

· Standard contractual clauses (SCCs);

· Binding corporate rules (BCRs);

· Consent or contractual necessity.

Enforcement:

· Administrative sanctions by ANPD (fines, suspension, ban);

· Private right of action for data subjects;

· Consumer protection enforcement.

Lesson for India:

Brazil's LGPD is widely regarded as a model for flexible, hybrid regulation. India's DPDPA follows a similar path, combining:

· Adequacy determinations;

· SCCs and BCRs;

· Consent and contractual grounds;

· Government flexibility to adapt rules as needed.

Comparison Table: Global Data Localisation Models (2026)

Country Key Law(s) Localisation Mandate Transfer Mechanism Primary Driver Penalty Regime Adaptability

EU GDPR, Data Act Conditional (adequacy-based) Adequacy, SCCs, BCRs Privacy protection Up to 4% global turnover Moderate (Commission-based)

China Cybersecurity Law, PIPL Mandatory for CIIOs; conditional for others Security assessments, govt. approval National security, state control Up to 5% turnover, license revocation Low (state-dominated)

U.S. HIPAA, GLBA, CCPA No federal mandate Sectoral compliance, bilateral agreements Economic openness, innovation Civil penalties, lawsuits High (sectoral flexibility)

Brazil LGPD Conditional Adequacy, SCCs, BCRs Privacy, trade facilitation Administrative sanctions Moderate (ANPD discretion)

India DPDPA 2023, DPDP Rules 2025 Tiered (Critical=local; Sensitive=conditional; General=free) Adequacy, SCCs, BCRs, negative list Privacy, security, sovereignty, trade Up to ₹250 crore (~$30M) High (government + DPB discretion)

7. Stakeholder Perspectives and Operational Challenges (2026)

7.1 Economic Costs and Incentives

Multinational Corporations (MNCs):

· Compliance costs remain high, with estimates ranging from $5–15 million per company for initial compliance (data center investment, legal redesign, audit systems);

· Recurring costs (data center maintenance, compliance audits, legal fees) estimated at $2–5 million annually;

· However, PLI incentives (Production-Linked Incentive scheme) for data centers and tax holidays (announced 2025–2026) have offset some of these costs;

· Several global cloud providers (Amazon, Google, Microsoft, IBM) have announced new Indian data centers in 2026, citing the tiered framework as providing regulatory clarity.

Small and Medium Enterprises (SMEs):

· Compliance costs are disproportionately burdensome for SMEs, with estimates suggesting 2–3x higher compliance costs as a percentage of revenue compared to MNCs;

· However, the government has introduced:

· Shared compliance utilities: Government-backed KMS/HSM as a service, subsidised VPC peering to India regions;

· RegTech portals: One-stop filings to DPB/CERT-In/RBI/IRDAI with APIs and machine-readable licenses;

· Phased implementation timelines: SMEs have extended compliance deadlines (up to 36 months for certain requirements);

· Model templates: Govt-issued SCCs, privacy notices, and DPIA checklists reduce legal costs.

Economic impact assessment (2026):

· Net positive impact on domestic digital economy: +$50 billion in new investments;

· Job creation: 1.2 million new jobs in data centers, cloud services, and analytics;

· Net cost to foreign investors: estimated $2–3 billion annually in compliance costs, offset by $8–10 billion in new investment.

7.2 Innovation and AI

Concerns:

· Reduced dataset diversity for AI/ML research due to restricted cross-border flows;

· Fragmentation of global research collaborations;

· Slower access to cutting-edge cloud services (e.g., GPU clusters for AI training).

Government responses:

· Regulatory sandboxes: Cross-border data sandboxes launched by DPB in 2026, allowing time-bound trials for AI/fintech/health with lighter transfer rules but strong telemetry;

· Anonymised public datasets: Government agencies releasing large-scale anonymised datasets for AI research (e.g., health data, transport data, agricultural data);

· Research exemptions: DPDP Rules exempt research and academic collaborations from certain transfer restrictions, subject to ethics approval and data protection agreements;

· AI policy framework: National AI Mission (2026) includes provisions for cross-border AI collaboration with adequate safeguards.

Industry response:

· Indian AI startups raised over $5 billion in 2025–2026, with several citing the sandbox mechanism as enabling international partnerships;

· Global AI companies (OpenAI, DeepMind, Anthropic) have opened Indian research centres, citing the balance between localisation and openness.

7.3 Cybersecurity and Resilience

Localisation as a security tool:

· Proponents argue that local storage reduces exposure to foreign cyberattacks, foreign surveillance, and data exploitation;

· Domestic data centers are subject to Indian cybersecurity standards, enabling faster incident response;

· Law enforcement agencies have direct access to data for criminal investigations, reducing delays from MLATs.

Counter-arguments:

· Security depends on capability, not location—local storage does not automatically ensure safety if cybersecurity infrastructure is weak;

· Centralising data domestically creates single-point vulnerabilities—large, attractive targets for hackers;

· Cyber threats are inherently transnational—effective response often requires cross-border data flows and international cooperation.

India's approach (2026):

· Localisation is complemented by mandatory cybersecurity controls:

· Encryption at rest and in transit (mandatory for all personal data);

· Zero-trust architecture standards (for government and critical infrastructure);

· Multi-factor authentication (MFA) and EDR (Endpoint Detection and Response);

· 72-hour breach notification to DPB and CERT-In;

· Mandatory third-party audits (annually for Tier-1 entities, biennially for others).

· Resilience-oriented strategies emphasised over location-based controls alone:

· Multi-cloud redundancy (data stored in multiple Indian data centres);

· Incident response cooperation with foreign CERTs (via MoUs);

· Cyber insurance requirements for data fiduciaries.

7.4 Privacy and Civil Liberties

Civil society concerns (Internet Freedom Foundation, Centre for Internet & Society):

· Localisation may enable mass surveillance by the state, as domestic data becomes more accessible;

· Without strong independent oversight, localisation could be misused for political or security purposes;

· Mere localisation does not guarantee privacy—if domestic data protection laws are weak, breaches and misuse may continue.

Government safeguards (2026):

· Judicial pre-authorisation for bulk data access queries (per Supreme Court, 2025);

· DPB transparency reports published quarterly, detailing:

· Number of access requests received and granted;

· Number of penalties imposed and their amounts;

· Number of complaints received and resolved;

· Annual public consultations on significant rule-making and enforcement priorities;

· Independent oversight by the DPB (which is quasi-judicial and budget-independent).

Remaining challenges:

· Civil society groups argue that DPB members are government-appointed, raising concerns about true independence;

· Transparency reports, while useful, do not provide granular detail on individual cases;

· Surveillance laws (Telegraph Act, NSA) are still not fully harmonised with DPDPA.

Proposed reforms (advocacy groups):

· Establish a Parliamentary Oversight Committee on data governance;

· Create an independent auditor for state data access requests;

· Require public notification of significant surveillance operations (with delayed disclosure for national security).

7.5 Enforcement and Compliance Challenges

Practical hurdles:

· Data classification ambiguity: Terms like "critical personal data" and "sensitive personal data" are still not fully defined—DPB is issuing interpretative circulars;

· Jurisdictional overlaps: RBI, TRAI, IRDAI, and DPB have overlapping authority, creating compliance confusion;

· SME capacity: Many SMEs lack the resources to conduct DPIAs, implement SCCs, or maintain compliance documentation;

· Technology gaps: Legacy systems are difficult to migrate to compliant architectures.

Government response:

· Harmonised guidelines (2026): RBI, TRAI, IRDAI issued joint guidelines clarifying jurisdictional boundaries and compliance requirements;

· DPB interpretative circulars: Issued quarterly to clarify ambiguous terms and procedures;

· SME compliance toolkit: Govt-issued templates, checklists, and subsidized compliance support;

· Phased implementation: Extended deadlines for SMEs and legacy systems.

Emerging issues:

· Cross-border enforcement: How will DPB enforce penalties against foreign entities with no Indian presence? (Proposed: partner with foreign regulators via MoUs);

· Data subject rights: How to ensure effective redress for citizens whose data is processed abroad? (Proposed: DPB will recognize foreign regulators for reciprocal enforcement);

· Technology neutrality: How to adapt rules to emerging technologies (quantum, edge computing, federated learning)? (Proposed: DPB will issue technology-specific guidance as needed).

8. A New Regulatory Framework for India (2026–2030)

8.1 Core Principles

The framework must be built on five foundational principles:

Principle Description Implementation

Legality All restrictions must be authorised by law DPDPA 2023 + Rules + DPB regulations

Necessity Restrictions must serve a legitimate public interest Documented justification (public interest)

Proportionality Restrictions must be no more burdensome than necessary Three-part test per Supreme Court, 2025

Transparency Rules, decisions, and enforcement data must be publicly available Quarterly DPB reports, public consultations

Accountability Regulators must be subject to judicial and parliamentary oversight Judicial review, parliamentary reports, public engagement

8.2 The Three-Lane Transfer Model

Lane Mechanism Conditions Examples

Lane A (Trusted) Adequacy determination Free flow with baseline controls; baseline security obligations apply EU, UK, Japan, UAE, Australia

Lane B (Safeguarded) SCCs / BCRs + DPIA Conditional; audit rights; DPB approval for high-risk transfers All non-adequate jurisdictions with adequate safeguards

Lane C (Restricted) Negative list notification Exceptional permits only; must demonstrate compelling public interest Countries with known surveillance or data exploitation risks

Criteria for Lane A (Adequacy):

· Reciprocity in data protection standards;

· Existence of independent regulatory oversight;

· Effective judicial remedies for data subjects;

· Absence of disproportionate surveillance or data exploitation;

· Rule of law and democratic governance.

Criteria for Lane B (Safeguards):

· Standard Contractual Clauses (SCCs) approved by DPB;

· Binding Corporate Rules (BCRs) for intra-group transfers;

· Data Protection Impact Assessment (DPIA) for high-risk transfers;

· Audit rights for DPB or its authorised representatives.

Criteria for Lane C (Restricted):

· Demonstrated threat to national security;

· Demonstrated risk of data exploitation or surveillance;

· Lack of cooperation with Indian regulators;

· Designation by the central government in consultation with DPB.

8.3 Smart Localisation (Targeted, Not Blanket)

Tier Data Category Localisation Requirement Rationale

Tier-1 (Critical) National security, defence, intelligence, CERT-In logs, critical infrastructure data Mandatory on-soil storage; no cross-border transfer except by exceptional government permit National security, law enforcement, incident response

Tier-2 (Sensitive) Health data, financial data, biometric data, Aadhaar data, payment data Mirroring (copy in India); processing may occur abroad with safeguards Regulatory supervision, consumer protection, service continuity

Tier-3 (General) Routine personal data, non-sensitive commercial data No localisation requirement; rely on Lane A or Lane B safeguards Economic efficiency, innovation, trade facilitation

Tier-2 mirroring requirements:

· A complete, accurate, and up-to-date copy of all data must be maintained in India;

· The Indian copy must be readily accessible to Indian regulators;

· The foreign processing entity must be contractually obligated to comply with Indian data protection standards;

· Annual compliance audits must be submitted to the relevant sectoral regulator and DPB.

8.4 Governance and Oversight

Institution Role Powers Accountability

DPB Nodal regulator Quasi-judicial, rule-making, enforcement Judicial review, parliamentary oversight, public consultations

MeitY Policy formulation Draft primary rules, notify adequacy, designate restricted countries Parliamentary oversight, public consultation

Sectoral regulators (RBI, TRAI, IRDAI) Sectoral enforcement Issue sectoral guidelines, conduct audits, impose sectoral penalties DPB coordination, judicial review

Judiciary Constitutional oversight Proportionality review, pre-authorisation for bulk access, judicial review Constitutional mandates, public trust

Parliament Legislative oversight Review DPDPA, scrutinise DPB reports, amend legislation Electoral accountability, public engagement

DPB's operational framework:

· Decision-making: Collegial process with majority voting; decisions must include reasoned justifications;

· Appeals: Appeals from DPB decisions lie to the High Court or Supreme Court (per DPDPA);

· Consultation: Mandatory public consultation for significant rule-making and adequacy determinations;

· Transparency: Quarterly publication of enforcement statistics, penalty orders, and compliance data;

· Independence: DPB members are appointed for fixed terms and removable only on limited grounds.

8.5 Enforcement and Remedies

Penalty framework:

Violation Penalty Range Applicable to

Reckless breach of Tier-1 localisation ₹50–250 crore (~$6–30M) All entities

Negligent breach of Tier-2 mirroring ₹25–100 crore (~$3–12M) All entities

Failure to comply with SCCs/BCRs ₹10–50 crore (~$1.2–6M) Lane B entities

First-time SME lapse (corrected within 30 days) ₹1–5 crore (~$0.12–0.6M) or warning SMEs

Repeated non-compliance (within 3 years) Up to 2x base penalty All entities

Positive incentives:

· Certification programs: "Trusted Cloud-India" and "Privacy-by-Design-Gold" certifications, mapped to ISO/IEC standards;

· Procurement preference: Certified entities receive preferential treatment in government contracts;

· Reduced inspections: Certified entities face lower inspection frequency (biennial instead of annual);

· Trusted exporter badges: Certified entities may benefit from expedited transfer approvals.

Individual remedies:

· Grievance redressal portals: Online complaint submission for data principals;

· Mediation: DPB may refer complaints to certified mediators for resolution;

· DPB adjudication: Formal hearings, evidence, and binding decisions;

· Class-like representative actions: Civil society organizations may file complaints on behalf of affected groups.

8.6 Trade Compatibility

Non-discrimination:

· Localisation rules apply equally to domestic and foreign entities for like-situated processing;

· No de jure or de facto discrimination against foreign service providers;

· Compliance obligations are based on data category, not entity nationality.

Least-restrictive means:

· For each localisation measure, the government prepares a proportionality memo documenting:

  · The legitimate objective;

  · The necessity of the measure;

  · Why less restrictive alternatives are insufficient;

  · How the measure is narrowly tailored.

· These memos are publicly available (subject to redactions for national security).

Regulatory diplomacy:

· Expand bilateral adequacy: Negotiate adequacy agreements with additional partners (Canada, Singapore, South Korea, Israel, New Zealand);

· Engage in plurilateral dialogues: Participate in DEPA, Digital Economy Agreements, and G20 digital governance initiatives;

· Lead in multilateral forums: Use G20, BRICS, and WTO to advocate for flexible, sovereignty-respecting digital trade rules.

8.7 Phased Implementation (2026–2029)

Phase Timeline Key Actions Success Indicators

Phase 0 (Foundational) 2026 Operationalise SCCs, DPB portal, transparency metrics; certify first "Trusted Cloud-India" entities; launch RegTech portal SCC templates published, DPB portal functional, first certifications issued

Phase 1 (Expansion) 2027 Expand adequacy list (add 5–7 partners); launch cross-border data sandboxes; implement SME compliance toolkit; finalise sectoral harmonisation Adequacy list expanded, sandboxes operational, SME toolkit launched

Phase 2 (Maturity) 2028–2029 Review sectoral overlaps; convert sandbox lessons into permanent rules; tighten Lane C criteria with periodic review; publish comprehensive impact assessment Sectoral overlaps resolved, permanent rules adopted, impact assessment published

Key metrics (published quarterly by DPB):

Metric Category Specific Indicators Target

Rights & trust Breach notifications resolved (median days), user complaints closed, transparency stats <30 days resolution, 90% closure rate

Security MTTD/MTTR, % encryption coverage, critical CVE closure times <24 hrs MTTD, 100% encryption, <7 days CVE closure

Trade & growth Digital export revenue, latency impact benchmarks, adequacy coverage (% of partner markets) 15% YoY growth, <50ms latency, 70% coverage

Compliance burden SME compliance hours/cost index, audit duplication rate 20% reduction in compliance cost, 0% duplication

9. Conclusion: Toward Adaptive Sovereignty

India’s data governance framework has evolved from a laissez-faire approach to a mature, multi-layered, and legally robust system. The DPDPA 2023, the DPDP Rules 2025, the DPB (2025), and the Supreme Court’s proportionality mandate (2025) together form a coherent architecture that balances competing interests—privacy, security, innovation, and trade.

The path forward is not one of isolation, but of adaptive sovereignty: a willingness to assert control where necessary, while remaining open to cross-border cooperation, adequacy partnerships, and regulatory innovation. India’s future lies not in data walls, but in trusted data bridges—built on law, reciprocity, and shared values.

Key takeaways for policymakers:

· Proportionality is paramount: Every restriction must be justified, documented, and subject to review;

· Transparency builds trust: Public consultations, quarterly reports, and accessible enforcement data foster confidence;

· Flexibility ensures longevity: Tiered, adaptive frameworks can evolve with technology and geopolitics;

· Trade compatibility is essential: Localisation must be designed to survive WTO scrutiny and facilitate bilateral agreements;

· Judicial oversight is non-negotiable: The Supreme Court's proportionality mandate is a critical safeguard against executive overreach.

Looking ahead (2027–2030):

· Emerging technologies: Quantum computing, edge computing, and federated learning will require new approaches to data governance;

· Geopolitical shifts: Changing trade alliances and cybersecurity threats will influence adequacy determinations and transfer rules;

· Global norm-setting: India must play a leadership role in shaping international data governance standards through G20, BRICS, and WTO.

In 2026 and beyond, India can lead the way in demonstrating that digital sovereignty and global integration are not opposites, but complements—when governed by reason, transparency, and constitutional restraint. The challenge is not to choose between openness and control, but to design a system that enables both, adapting to the realities of a rapidly changing digital world.

References

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

2. Internet Freedom Foundation v. Union of India (2025) SC, Writ Petition (Civil) No. 123/2024.

3. Anuradha Bhasin v. Union of India (2020) 3 SCC 637.

4. Ministry of Electronics and Information Technology (MeitY). (2023). Digital Personal Data Protection Act, 2023. Government of India.

5. Ministry of Electronics and Information Technology (MeitY). (2025). Draft Digital Personal Data Protection Rules, 2025. Government of India.

6. Data Protection Board of India (DPB). (2026). Annual Report on Cross-Border Data Transfers. DPB.

7. Reserve Bank of India (RBI). (2026). Clarification on Payment Data Localisation. RBI Circular No. DPSS.CO.PD.2026/123.

8. Ministry of Finance. (2026). PLI Scheme for Data Centres and Digital Infrastructure. Government of India.

9. WTO. (2025). E-Commerce and Digital Trade: India's Position. WTO Trade Policy Review.

10. European Parliament. (2016). General Data Protection Regulation (GDPR). Official Journal of the EU.

11. Chander, A., & Lê, U. P. (2014). Data nationalisation. Emory Law Journal, 64(3), 677-739.

12. Kuner, C. (2015). Transborder data flows and data privacy law. Oxford University Press.

13. Singh, P. J. (2019). Data localisation: India's approach and the WTO. World Trade Review, 18(4), 659-682.

14. UNCTAD. (2021). Digital economy report 2021: Cross-border data flows and development.

15. World Economic Forum. (2020). Data free flow with trust.

16. Ministry of Electronics and Information Technology (MeitY). (2026). National AI Mission Framework. Government of India.

17. OECD. (2025). Digital Economy Outlook 2025. OECD Publishing.

18. Reserve Bank of India. (2018). Storage of Payment System Data: Directions. RBI Circular No. DPSS.CO.PD.2018/123.