

5. Digital Sovereignty – Polity

Global power structures have shifted from control over physical assets (oil, chokepoints) to Digital sovereignty. A nation's digital footprint is now the primary source of wealth and the most effective tool of diplomacy

Digital Sovereignty – Digital Sovereignty refers to a nation's ability to exercise full control over its digital infrastructure, data flows, digital platforms, and cyberspace regulation without external interference. It is a multi-layered framework spanning –

- 1. Physical Layer** – Hardware, servers, cloud infrastructure, data centres, telecommunication networks, semiconductor fabrication, fiber optic cables.
- 2. Code Layer** – Algorithms, standards, protocols, encryption policies, software architecture, AI models.
- 3. Data Layer** – Ownership, storage, cross-border flows, governance, privacy, and processing of personal and non-personal data. The larger objective is to ensure that India—not foreign governments or corporations—determines how Indian data, digital systems, and online interactions are governed.

Pillars of Digital Sovereignty

1. Data Sovereignty – Data generated within India is –

- 1. Stored within Indian borders
- 2. Processed under Indian laws
- 3. Accessible to Indian regulators, not foreign governments

Crucial for national security and privacy.

2. Technological Sovereignty – Ability to develop and maintain –

- 1. Indigenous chips (semiconductors)
- 2. 5G/6G telecom systems
- 3. AI models (Bhashini-like LLMs)
- 4. Secure cloud services
- 5. Cybersecurity tools

Reduces dependence on US/China tech monopolies.

3. Platform Sovereignty – Encouraging Indian alternatives to –

- 1. Social media platforms
- 2. E-commerce marketplaces
- 3. Digital payments systems

Enables control over content moderation, data storage, and platform governance.

4. Cyber Sovereignty – Ensuring the nation's cyberspace is secure, monitored, and governed through –

- 1. CERT-In advisories
- 2. National Cyber Security Strategy (proposed)
- 3. Cybercrime investigation units

Prevents cyber warfare and foreign interference.

5. Regulatory Sovereignty – Ability to make independent digital rules that protect national interests, regardless of global tech lobbying or foreign pressure.

Why Digital Sovereignty Matters for India

1. Massive and Growing Digital Footprint – India is one of the world's largest data ecosystems –

- 1. Over 800 million internet users
- 2. World's 2nd-largest smartphone market
- 3. Digital economy projected to reach \$1 trillion by 2025–26

Huge user bases → massive personal and behavioural data → high vulnerability.

2. National Security Imperatives – When Indian data is stored abroad, it can be –

1. Accessed by foreign intelligence agencies
2. Subject to foreign laws (e.g., U.S. CLOUD Act)
3. Vulnerable to geopolitical coercion

Localisation ensures data remains under India's jurisdiction.

3. Rising Cyber Threats – India faces –

1. Ransomware attacks
2. Deepfake misinformation campaigns
3. Financial fraud
4. State-sponsored cyber intrusions

Localised data enables faster auditing, better monitoring, and improved response times.

4. Economic Opportunities – Data localisation encourages –

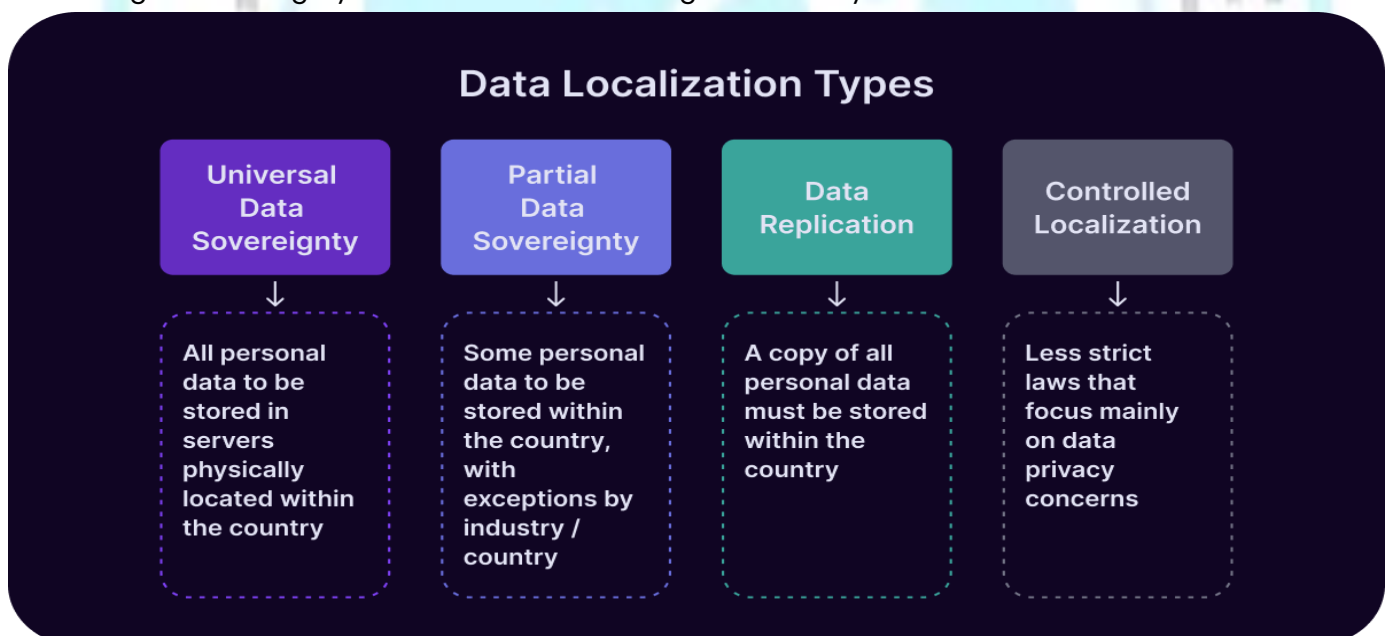
1. Growth of domestic data centres
2. Cloud computing industries
3. AI and analytics companies
4. Skilled jobs in cybersecurity, chip design, DevOps

Builds a strong indigenous digital economy.

5. Global Power Dynamics – Nations with control over digital ecosystems become –

1. Rule-makers (not rule-takers)
2. Influential in global tech standards (AI governance, encryption norms)

Digital sovereignty is linked to overall strategic autonomy.



Challenges to Digital Sovereignty

1. Big Tech Dominance – India heavily depends on foreign firms for –

1. Search engines
2. Social media
3. Cloud computing
4. E-commerce
5. Operating systems
6. Creates risks of monopolistic control and regulatory resistance.

2. Technological Dependence – India imports –

1. Semiconductors

2. Telecom equipment
3. Cloud infrastructure
4. AI hardware accelerators

Limits long-term digital autonomy.

3. Borderless Nature of the Internet – Hard to regulate cross-border digital flows. Data often travels through multiple jurisdictions on global cloud systems.

4. Impact on Global Business – Strict data localisation may –

1. Increase compliance costs
2. Reduce ease of doing business
3. Restrict innovation
4. Discourage foreign investment

Needs careful, calibrated implementation.

5. Skilled Workforce Gaps – Shortage in areas such as –

1. Cybersecurity
2. AI/ML
3. Chip fabrication
4. Quantum computing
5. Ethical hacking

Slows progress towards technological sovereignty.

Government Initiatives Supporting Digital Sovereignty

1. Digital Competition Bill (Draft 2024) – Targets Big Tech gatekeeping. Addresses –

1. Self-preferencing
2. Data monopolies
3. Predatory pricing
4. Anti-competitive bundling

Promotes fair digital markets.

2. Digital Personal Data Protection (DPDP) Act, 2023 – Establishes –

1. Consent-based data governance
2. User rights
3. Penalties for data misuse
4. Obligations for data fiduciaries

Strengthens privacy and data autonomy.

3. Competition (Amendment) Act, 2023 – Enhances CCI's power to rapidly curb anti-competitive conduct in digital markets. Focus on digital mergers, killer acquisitions, and monopoly behaviour.

4. IT Rules, 2021 – Requirements for platforms –

1. Traceability
2. Content moderation transparency
3. User grievance officers
4. Compliance reporting

Strengthens platform accountability.

5. Open Network for Digital Commerce (ONDC) – Reduces dependence on Amazon/Flipkart-type platforms. Builds open, interoperable e-commerce infrastructure.

6. Digital India Initiative – Promotes –

1. Universal digital access
2. Digital literacy

3. Cybersecurity
4. Citizen empowerment

Forms the backbone of India's sovereign digital ecosystem.

Way Ahead

1. Balance Sovereignty with Openness – India must avoid a closed internet model like China's; Aim for secure openness that safeguards data while enabling global trade.

2. Privacy as a Fundamental Right – Digital framework must align with –

1. Puttaswamy (2017) judgment
2. Individual dignity
3. Ethical data practices

3. Transparent Big Tech Regulation – Prevent dominance without stifling innovation. Ensure rules are fair, predictable, and democratically accountable.

4. International Cooperation – Secure data transfer agreements (like EU's GDPR-based mechanisms). Develop joint cyber defence frameworks. Set global rules on AI ethics, algorithmic transparency, and data flows.

5. Build Indigenous Capabilities – Invest in –

1. Chip manufacturing (Semicon India)
2. National cloud (MeghRaj)
3. Indian LLMs
4. Cybersecurity workforce
5. Quantum tech

Reduces foreign dependence and strengthens economic sovereignty.

Conclusion

Digital Sovereignty is essential for ensuring that India—not external actors—control its digital assets, data, and online ecosystem. As India becomes a global digital powerhouse, safeguarding data, regulating platforms, and building indigenous digital capacity will be essential for national security, economic growth, and democratic accountability. India's approach must balance sovereignty, openness, innovation, and privacy, shaping a resilient and future-ready digital governance framework.

Source – <https://indianexpress.com/article/opinion/columns/shashi-tharoor-writes-india-must-choose-digital-sovereignty-or-submit-to-the-new-subtle-digital-raj-10388173/>