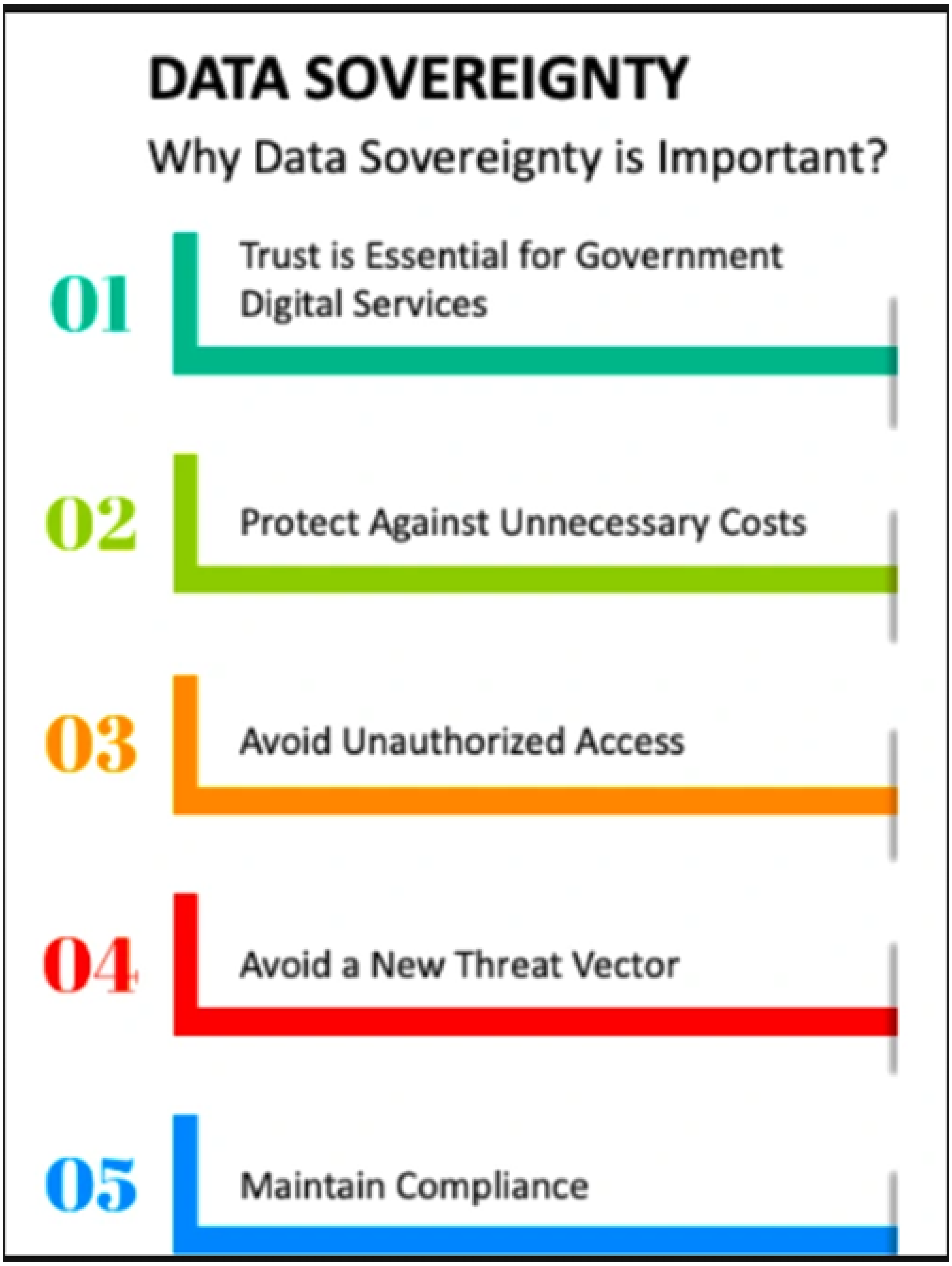
DIGITAL SOVEREIGNITY

Published On: 02-08-2025

What is digital sovereignty?

Digital sovereignty, cyber sovereignty, technological sovereignty and data sovereignty refer to the ability to have control over your own digital destiny – the data, hardware and software that you rely on and create.

Prime Minister Narendra Modi emphasized the need for **collective global efforts at the AI Action Summit in Paris.**



DATA SOVEREIGNTY

Why Data Sovereignty is Important?

01 Trust is Essential for Government Digital Services

02 Protect Against Unnecessary Costs

03 Avoid Unauthorized Access

04 Avoid a New Threat Vector

05 Maintain Compliance

Reasons for the rising significance of digital soverignity

l**National Security Imperatives:**

Dependence on foreign hardware, software, and critical digital infrastructure creates vulnerabilities for espionage, sabotage, and cyber warfare. Nations want to secure their digital borders.

Example: The Semiconductor Mission (ISM), aiming for indigenous chip manufacturing, is a direct response.

l**Economic Competitiveness and Value Creation:**

Reason: Control over data and technology allows nations to foster domestic innovation, create jobs, and ensure that economic value generated from digital activities stays within their borders rather than flowing to foreign tech giants.

Example: The "Make in India" and "Atmanirbhar Bharat" initiatives vigorously promote local manufacturing of electronics and IT hardware.

l**Data Privacy and Protection of Citizens' Rights:**

Reason: Growing concerns over mass surveillance, data breaches, and the misuse of personal data by foreign entities or dominant tech companies necessitate strong national data protection laws.

Example: The Digital Personal Data Protection Act (DPDP Act), 2023, even with its flexibility on cross-border data transfers, emphasizes data principal rights.

l**Geopolitical Leverage and Strategic Autonomy:**

Reason: Digital capabilities are increasingly a tool of state power. Nations seek to avoid being digitally subservient to other global powers or technological monopolies, especially during geopolitical tensions.

Example: The government's ban on numerous Chinese apps (e.g., TikTok in 2020) demonstrated India's willingness to exercise its digital autonomy.

l**Ethical AI Development and Governance:**

Reason: As Artificial Intelligence becomes more pervasive, nations want to ensure that AI systems developed and deployed within their borders align with their societal values, ethical principles, and regulatory frameworks, rather than being dictated by foreign standards.

Example: While still evolving, India's discussions around responsible AI, data governance.

Challenges in securing digital soverignity

Securing digital sovereignty presents a complex array of challenges for any nation, and India, despite its ambitious strides, faces significant hurdles.

High Costs and Investment in Critical Infrastructure: Building self-sufficient ecosystems for semiconductors, advanced computing, and data centers requires enormous capital investment, specialized machinery, and long gestation periods.

Lack of Domestic Expertise and Talent Pool (Deep Tech): While India has a vast pool of IT talent, specialized skills in areas like chip design, advanced materials science, cybersecurity research, and ethical AI development are still relatively nascent or insufficient for true self-reliance.

Global Dominance of a Few Tech Giants (Vendor Lock-in): The digital landscape is largely shaped by a handful of global technolog companies (from the US and China) that control operating systems, cloud infrastructure, AI models, and major social media platforms. Breaking free from this vendor lock-in is extremely difficult.

Balancing Digital Sovereignty with Global Trade and Investment: Imposing strict data localization or technology restrictions can be seen as protectionist measures, potentially deterring foreign investment and hindering India's participation in global digital trade frameworks.

Cybersecurity Threats and Evolving Attack Surfaces: Despite efforts to secure digital assets, the increasing sophistication and frequency of cyberattacks (ransomware, state-sponsored attacks, data breaches) pose a continuous threat to national data and critical infrastructure.

Steps taken by india for digital soverignity

Digital Personal Data Protection Act, 2023: To replace India’s existingInformation Technology Act of 2000and provide comprehensive oversight of the digital landscape. It seeks to address modern challenges likecybercrime, data protection, deepfakes and online safety.

New Information Technology (Intermediary Guidelines) Rules 2021: Intermediary Guidelines Ruleswith more stringent content moderation rules for online platforms, making numerous references to the protection ofIndia’s sovereignty and integrity

Development of Digital Public Infrastructure (DPI) - India Stack: India has consciously built robust public digital infrastructure like Aadhaar, UPI, and DigiLocker, which are open, interoperable, and domestically owned/controlled. This provides a national digital backbone, reducing dependence on foreign private platforms for core public services.

Data Localization in Specific Sectors: Even with the DPDP Act's more flexible approach to cross-border data flows, certain critical sectors in India have long had or continue to enforce specific data localization mandates for national security and regulatory oversight.

Strategic Autonomy in Digital Governance: India actively seeks to shape global digital governance norms, advocating for a multilateral, multi-stakeholder approach rather than being a passive recipient of rules set by dominant digital powers.

Promotion of Domestic Cloud Solutions and Data Centers: Recognizing the importance of cloud infrastructure, India is encouraging the development of indigenous cloud platforms and data centers to ensure data residency and reduce reliance on hyperscale foreign cloud providers.

Way Forward to the Digital Sovereignty

Adopting a Flexible Approach: India need not to follow an ‘all or nothing’ deal that forces it to adopt consensus-based rule-making on all issues of digital trade. Instead, India should push for the modular approach adopted by the Digital Economy Partnership Agreement (DEPA) between Singapore, Chile and New Zealand.

Promoting Alternative Indian Platforms like:

Koo: Koo is an Indian microblogging and social networking platform launched with a focus on Indian languages and a government-friendly stance, as an alternative to X (formerly known as Twitter).

BharatOS: A mobile operating system to challenge Google whose Android operating system (OS) dominates the country’s smartphone market.

Open Network for Digital Commerce (ONDC): It displays products and services from member e-commerce platforms, and is touted as an alternative to Amazon and Walmart.

Ideological Mediation: Nations across the globe have differing interpretations of digital sovereignty, with the third way which appropriately regulating multinational companies to further public interest while still championing civil liberties online and cross-border data flows with minimal restrictions.