Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2025 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Digital Sovereignty and India's Data Dilemma

Vedika[a]

[a]National University for Study and Research in Law, Ranchi, India

Received 11 January 2025; *Accepted* 12 February 2025; *Published* 17 February 2025

The increasing integration of digital technologies in global economies has led to the growing importance of digital sovereignty, a concept central to the governance of data and its flows across borders. As India's growth in the digital economy has unfolded, the conflict between securing national interests and staying engaged in the global data ecosystem has been sharpened. The country's effort in dealing with cross-border data transfer, privacy concerns, and regulatory framework represents a deeper and broader international debate on balancing the control over digital resources and international cooperation. This article takes a closer look at India's changing stance on digital sovereignty through its legal frameworks for data protection, privacy, and cybersecurity. The article discusses the implications of emerging law and the challenges posed by foreign digital platforms in collecting and processing Indian citizens' data. The article also examines the tension between India's push for data localization and the global push for free data flow in the context of international trade and the digital economy. Comparative Data Sovereignty Approaches between and among regions indicate this article highlights all the challenges with which India should manoeuvre its quest to assert its data sovereignty amidst enhancing global digital engagement. With evaluations of legal-political-economic rationales, this paper seeks to support the ongoing debate as it tries to shed light on which approach can most effectively be able to take a step out while ensuring its continued digital sovereignty would not dismember it from participating in the mainstream global digital realm.

Keywords: *digital sovereignty, data protection, data localization, cybersecurity, cross-border flow.*

INTRODUCTION

The age we live in is that of unprecedented technological advancement and one of the most prominent questions that arise concerning such a setting is the question of who controls the data. Data has been referred to more frequently as 'the new oil' - similar to a rare and precious fuel that pervades businesses and is important to produce substantial benefits involving the core requirement of a business such as analytics or to meet the demands of the future like artificial intelligence. In the year 2017, an article observed that the world's most valuable resource is no longer oil, but data.[1] Hence, therefore it is not so far-fetched to say that data forms the lifeblood of the digital economy and has been gaining momentum as a central component of global politics, economics, and security. Countries across the globe, including India, are in a delicate situation of how they can embrace all the opportunities which the globalised digital economy holds for them on one hand, while ensuring all their sovereignty remains intact in cyberspace. Such an interplay where nations are interconnected yet still maintain sovereignty has led to the formation of the concept of 'Digital Sovereignty', referred to as the ability of a nation-state to regulate and control its digital assets, data flows, and infrastructure.

Digital sovereignty is more than just control over data; it encompasses setting regulations in how technologies operate within a nation's borders and how cross-border data flows are managed or ordered. It also encompasses how international norms relating to digital trade are negotiated. The multifaceted concept of digital sovereignty subsumes data protection and cybersecurity as encompassing autonomy in technological innovation along with resilience against foreign interference. With the further advancement of technologies affecting and influencing crucial sectors, such as health, defense, finance, and education, nations are vulnerable to external dependencies as well as cyber-attacks in the absence of digital sovereignty.

Data processing and collection are governed by the provisions and policies of the country from where the data originated. The urgency of this issue is more apparent than ever, as nations

[1] Deepak Thakur, 'Data Sovereignty: Here's How Critical It Is for India's Digital Roadmap' *Economic Times* (10 October 2022) <https://cio.economictimes.indiatimes.com/news/strategy-and-management/data-sovereignty-heres-how-critical-it-is-for-indias-digital-roadmap/94750605> accessed 03 January 2025

implement stringent data localization laws, negotiate international treaties on data governance, and develop modern cybersecurity norms. For India, a burgeoning digital powerhouse, stakes are especially high. In the fight against 'Digital Colonialism'- a practice of extracting and controlling data from individuals without their consent,[2] India has been one of the most active and outspoken members of data sovereignty[3]. India's aspirations for self-reliance and self-dependence especially in the field of technology intersect with its deep integration into the global data ecosystem. This is the reason digital sovereignty is not just a matter of national interest but a linchpin of India's economic and strategic future.

Indian digital sovereignty is very much beyond economic significance and relates to far broader aspects such as geopolitics and strategy. It would become much more relevant for India if it not only reacts to the mighty structures implemented by global powers like the United States, China, and the European Union (EU) but also prepares its own approach well in advance so as not to find itself as an uncritical follower of the emerging new world order. A strong approach towards digital sovereignty will help India ensure that foreign entities comply with domestic regulations, protect sensitive data from external exploitation, and foster innovation in indigenous technology.

THE CONCEPT OF DIGITAL SOVEREIGNTY

Digital sovereignty is a term coined recently, however, when viewed deeper, its origins are embedded in the very broader concept of state sovereignty, which has emerged since the Treaty of Westphalia in 1648, as a constitutive principle of international law.[4] Traditionally, sovereignty is defined as a state's domination over territory, laws, and governance. As the world evolves into a digital age, sovereignty has been expanded to include the control of a nation over digital assets, data, and infrastructure.[5] The evolution of digital sovereignty gained momentum in the

[2] Michael Kwet, 'Digital Colonialism Is Threatening the Global South' *Al Jazeera* (13 March 2019) <https://www.aljazeera.com/opinions/2019/3/13/digital-colonialism-is-threatening-the-global-south> accessed 03 January 2025
[3] Thakur (n 1)
[4] Riadhotul Muamalah, 'Evolution of International Law: From Early Treaties to Concept of Contemporary Sovereignty' (2025) 2(1) Aliansi: Jurnal Hukum, Pendidikan Dan Sosial Humaniora <https://doi.org/10.62383/aliansi.v2i1.671> accessed 03 January 2025
[5] *Ibid*

contemporary age as a result of the growth of technology and the internet. This led to nations recognizing that cyberattacks, foreign surveillance revelations and the rise of global technology giants are major concerns over national control in cyberspace and data could prove to be of strategic importance as an economic resource and a powerful tool for political influence.

Digital sovereignty is built over three essential and interrelated principles- data localization, privacy, and national security. Data localization mandates that a given data when developed within a nation's territorial borders should be domestically stored and processed. This principle forms the core of digital sovereignty as it ensures that sensitive data remains subject to local laws. For India, initiatives like the Digital Data Protection Act[6] propose varying degrees of data localization, aimed at reducing dependence on foreign entities and safeguarding critical information.[7] Second is privacy, which is both an inalienable right and the bedrock of digital sovereignty. Among the primary responsibilities of a nation is to safeguard the private lives of its citizens from abuse and exploitation and hence the nations focus more on frameworks that protect privacy. In India's case, the issue of privacy was debated over and established as one of rights, as in Puttaswamy, which stoked legislative activities to establish serious privacy protections for the challenges regarding cross-border flows of data.[8] National security is the last but not the least. Digital infrastructure is now integral to all the critical sectors of defence, economy, education, and healthcare. Therefore, ensuring national security becomes a priority. Digital sovereignty helps states in reducing risks such as cyberattacks, espionage, and manipulation of information by having control over their digital ecosystem.

The debate about digital sovereignty mainly centres on the balance between digital openness, and regulation over the spread of data across the continents as it fosters global trade, innovation, and collaboration. Digital openness most often sees a curb on data flow as a hindrance to economic growth and technological development. Digital sovereignty, on the other hand, emphasizes the need for control of the digital landscape of nations to realize privacy, security,

[6] Digital Personal Data Protection Act 2023
[7] 'How Data Sovereignty and Localisation Impact Privacy Programmes' (*Protiviti*) <https://www.protiviti.com/in-en/insights-paper/how-data-sovereignty-and-localisation-impact-privacy-programmes> accessed 03 January 2025
[8] 'Cross-Border Data Flows: Privacy and Compliance Considerations' (*OCR*, 24 April 2024) <https://www.ocr-inc.com/cross-border-data-flows-privacy-and-compliance-considerations/> accessed 03 January 2025

and local industry protection. The unregulated data flows and the foreign dominance over digital infrastructure undermine national interests, leaving countries vulnerable to exploitation. These conflicting views often lead to policy conflicts in situations where international frameworks like the World Trade Organization (WTO) push for liberated data flows, while countries like India seek to impose localization requirements to secure domestic interests. This conflict is deepened when the monopolistic power of global tech giants, which often operate beyond the regulatory reach of individual nations.[9]

INDIAN LEGAL FRAMEWORK FOR DATA PROTECTION

India's framework under law for data protection consists of statutes, sector-specific regulations, and judicial pronouncements. Although this framework is still being developed, it reflects the country's growing focus on balancing technological advancements with individual privacy rights.

The Information Technology (IT) Act, 2000 is the foundational statute of India's digital and data protection laws. Section 43A of the Act necessitates that corporate entities handling sensitive personal data or information (SPDI) adopt reasonable security practices. Failures to comply would result in compensation claims.[10]. Section 72 penalizes unauthorized disclosure of information obtained under the Act.[11] The IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, supplement the Act, defining SPDI and requiring consent and grievance redress mechanisms.[12]

The Digital Personal Data Protection Act, 2023 modernizes the traditional framework by establishing explicit data protection principles. It introduces a model of consent-based processing, ensuring all individual rights about data access, correction, and erasure. Accountability, breach notification, and a cross-border restriction of data transfers also form parts of the Act. India also has sector-specific regulations for data protection like Reserve Bank

[9] Arindrajit Basu, 'Sovereignty in a Datafied World' (*Observer Research Foundation,* 10 October 2021) <https://www.orfonline.org/research/sovereignty-in-a-datafied-world> accessed 03 January 2025
[10] Information and Technology Act 2000, s 43A
[11] Information and Technology Act 2000, s 72
[12] IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011

of India (RBI) enforces strict data security and localization norms for financial data while the healthcare sector has provisions under the Clinical Establishments Act, of 2010[13]. Similarly, telecom and insurance regulations mandate privacy safeguards and breach reporting mechanisms.[14]

Indian courts have time and again significantly influenced the evolution of data protection jurisprudence. The Hon'ble Supreme Court in the case of Justice K.S. Puttaswamy v UOI [15] established the 'Right to Privacy' as a fundamental right under Article 21 of the Constitution[16]. The judgment emphasized the need for stringent data protection laws that could safeguard individual privacy in the digital age.[17] In Faheema Shirin v Kerala State (2020), the Kerala High Court held that privacy rights extend to protecting individuals against state intrusion into their data.[18] The Hon'ble Supreme Court has repeatedly highlighted the need to ensure authenticity and privacy in handling electronic data, particularly in the context of evidence. Indian courts have also played an active role in addressing the corporate handling of personal data. In recent cases concerning data breaches, it has been emphasized that there is a need for accountability and adequate security measures along with creating de facto standards in the absence of comprehensive legislation.

CHALLENGES OF CROSS-BORDER DATA FLOWS IN INDIA

The cross-border flow of data is increasingly becoming a critical component of India's digital economy, but it also poses important legal, economic, and operational challenges. These issues often arise from debates on data localization, jurisdictional enforcement conflicts, and financial implications for trade, innovation, and foreign investment.

---

[13] Clinical Establishments Act 2010

[14] Shabih Fatima, 'Cross-Border Data Flow in India: An Analysis of the Digital Personal Data Protection Act, 2023 and General Data Protection Regulations, 2016' (2024) 4(3) International Journal of Advanced Legal Research <https://ijalr.in/wp-content/uploads/2024/02/Data-flow-research-paper.pdf> accessed 03 January 2025

[15] *Justice K.S. Puttaswamy (Retd.) and Anr v Union of India and Ors* (2017) 10 SCC 1

[16] Constitution of India 1950, art 21

[17] Pranav Rai, 'The Indian Supreme Court's Aadhaar Judgment: A Privacy Perspective' (*International Association of Privacy Professionals*, 09 October 2018) <https://iapp.org/news/a/the-indian-supreme-courts-aadhaar-judgement-a-privacy-perspective/> accessed 03 January 2025

[18] *Faheema Shirin v State of Kerala* (2020) 4 KerLJ 634

The storage of data within national borders is a means of enhancing sovereignty and security over data. Control over information in physical terms by governments would mean, among other things, better compliance with domestic laws and direct access during investigations by law enforcement agencies to given data. A significant demand that has led to this call is for national security and by the same token, protection of citizens' data from foreign surveillance[19]. On the other hand, data localization could lead to financial and operational challenges, especially for multinational corporations (MNCs) and startups. A huge cost for establishing local data centers in India would be incurred and might discourage foreign investment. The constraint, especially for startups, is their low capital base. Besides this, businesses argue that such mandates break the global internet, dislocating innovation and reducing competitiveness.[20] MNCs like Meta or Facebook along with Twitter have experienced operational hurdles under India's data localization framework. For instance, an Indian tribunal recently issued an antitrust order against WhatsApp and Meta, citing the tension between regulatory requirements and business operations. Fintech startups have also reported increased costs in compliance with localization mandates, which has hindered their scaling and innovation.[21]

Secondly, India often experiences jurisdictional conflicts in the regulation of cross-border data. Foreign entities may resist compliance with Indian laws if doing so violates their obligations in other countries. For instance, OpenAI informed India that removing ChatGPT training data could breach the legal obligations of the United States underscoring the complexities of enforcing national regulations on foreign corporations operating across multiple jurisdictions. [22]Furthermore, India faces significant hurdles in accessing data stored overseas. The lack of strong international agreements and data-sharing protocols prolongs access, which makes it

[19] Anirudh Burman and Upasana Sharma, 'How Would Data Localization Benefit India'' (*Carnegie Endowment for International Peace*, 14 April 2021) <https://carnegieendowment.org/research/2021/04/how-would-data-localization-benefit-india> accessed 03 January 2025

[20] Kalika Likhi, 'India's Data Localization Efforts Could Do More Harm than Good' (*Atlantic Council,* 01 February 2019) <https://www.atlanticcouncil.org/blogs/new-atlanticist/india-s-data-localization-efforts-could-do-more-harm-than-good/> accessed 03 January 2025

[21] Arpan Chaturvedi, 'India Tribunal Puts Antitrust Order on WhatsApp-Meta Data Sharing Ban on Hold' *Reuters* (23 January 2025) <https://www.reuters.com/technology/india-tribunal-puts-antitrust-order-whatsapp-meta-data-sharing-ban-on-hold-2025-01-23/> accessed 03 January 2025

[22] *Ibid*

even harder to tackle cybercrimes or digital investigations. These problems show the importance of streamlined global frameworks to allow cross-border cooperation.[23]

Lastly, India faces economic complications when dealing with cross-border data flow. Mandatory data localization can act as a non-tariff trade barrier and can discourage foreign businesses from investing in India. Setting up local data storage infrastructure is likely to raise costs for startups and MNCs significantly, thus possibly deterring it. This could then reduce India's competitiveness in the global digital economy and may open up trade disputes[24]. Furthermore, the high cost of compliance could restrict their ability to innovate, expand, and compete globally leading to a reduction in possibilities. Data localization requirements also limit opportunities for collaboration with international partners, further constraining growth in the Indian startup ecosystem.[25]

GLOBAL PERSPECTIVE

Indian approach towards data protection can benefit from examining global frameworks, especially the European Union (EU), the United States (US), and China.

The EU's General Data Protection Regulation (GDPR) is a comprehensive framework that governs data protection and privacy. It has stringent consent conditions, rights of data subjects, and hefty fines in case of non-compliance.[26] Cross-border transfers in the GDPR allow them to make transfers only if the destination country assures adequate levels of protection of their data. In case there are no such decisions of adequacy, the rights of the data subjects are protected by the SCCs or BCRs. Such an approach ensures personal data is processed in third countries with

[23] Smriti Parsheera and Prateek Jha 'Cross-Border Data Access for Law Enforcement: What Are India's Strategic Options?' (*Carnegie Endowment for International Peace*, 23 November 2020) <https://carnegieendowment.org/research/2020/11/cross-border-data-access-for-law-enforcement-what-are-indias-strategic-options> accessed 03 January 2025

[24] *Ibid*

[25] Alex Mathew, 'Cloud Data Sovereignty: Governance and Risk Implications of Cross-Border Cloud Storage'' (*ISACA*, 18 November 2024) <https://www.isaca.org/resources/news-and-trends/industry-news/2024/cloud-data-sovereignty-governance-and-risk-implications-of-cross-border-cloud-storage> accessed 03 January 2025

[26] General Data Protection Regulation 2016

strict control over it outside the EU so that high standards of privacy can be maintained around the world.[27]

The US adopts a sector-specific approach towards data protection, with regulations tailored to particular industries. For instance, the Health Insurance Portability and Accountability Act (HIPAA) governs healthcare data, while the Gramm-Leach-Bliley Act (GLBA) addresses financial data. This approach is patchwork, resulting in variable protections between and among sectors. The US has no federal data protection law on par with the GDPR of the EU, which is applied uniformly to the member states of the EU, thus leaving one loophole and then a discrepancy in privacy protections. However, Congress is now gaining the momentum to have a national standard of data privacy, which is a growing realization of the need for stronger and more uniform data protection.[28]

China enforces stringent data localization and control measures through laws like the Personal Information Protection Law (PIPL). Personal data collected within China must be stored domestically and impose strict conditions on transferring data abroad. The emphasis is on national security and maintaining sovereignty over data to ensure that the Chinese government retains control over data flows, but it also poses obstacles for multinational companies or MNCs operating in China, as they have to navigate complex compliance requirements to transfer data internationally.[29]

The data protection framework of India can draw valuable insights from these global approaches. Firstly, adopting a unified data protection law, similar to GDPR, can provide consistent and robust privacy safeguards. Secondly, stringent control can ensure data sovereignty however it is critical to balance these with flexibility to foster innovation and ease

[27] Thakur (n 1)
[28] Moira Warburton, 'Federal Data Privacy Laws Gain Support in US Congress, Critics Remain' *Reuters* (26 June 2024) <https://www.reuters.com/world/us/federal-data-privacy-laws-gain-support-us-congress-critics-remain-2024-06-26/> accessed 03 January 2025
[29] Thales, 'Global Data Sovereignty: A Comparative Overview' (Cloud Security Alliance, 06 January 2025) <https://cloudsecurityalliance.org/blog/2025/01/06/global-data-sovereignty-a-comparative-overview> accessed 03 January 2025

of doing business. Lastly, by incorporating sector-specific regulations, similar to the US approach, India can address the unique data protection needs of different industries.

BALANCING DIGITAL SOVEREIGNTY AND GLOBAL INTEROPERABILITY

In a strive to safeguard digital sovereignty, India needs to balance these efforts with the need for global interoperability to foster innovation, trade, and cooperation in the digital economy, especially in crafting policies that respect national interests while enabling seamless integration with the global data ecosystem.

Digital sovereignty is the ability of any nation to be in control of data created within its borders. Although it increases the security of data and adherence to domestic law, over-aggressive restrictions, such as what most realize today with data localization, stifle innovation and economic growth. There is, therefore, a middle ground. By adopting policies that place critical data within the jurisdiction while promoting the free flow of non-critical data across borders, countries can moderate their digital sovereignty[30]. For instance, India's Digital Personal Data Protection Act, 2023 seeks to relax localization requirements for non-sensitive data, so businesses can work globally while remaining sovereign over critical information. Embracing technological solutions like encryption, anonymization, and advanced data-sharing frameworks can bring sovereignty without suffocating innovation.

International frameworks play a critical role in reconciling national sovereignty with global data flows.[31] Agreements like the World Trade Organization's (WTO) provisions on e-commerce and trade pacts incorporating data protection clauses can facilitate cross-border data interoperability. An example of the same can be seen in the Japan- EU Economic Partnership Agreement in incorporating rules for data protection while enabling smooth data transfers, serving as a model for balancing privacy with trade interests. India could leverage its participation in forums like the G20 or bilateral agreements to advocate for a multilateral framework that ensures fair data access while addressing concerns related to sovereignty.[32]

---

[30] *Ibid*
[31] Luca Belli, *CyberBRICS: Cybersecurity Regulations in the BRICS Countries* (*Springer Nature* 2021)
[32] *Ibid*

Balancing digital sovereignty and global interoperability demands a nuanced approach that embraces cooperation, technological innovation, and stakeholder engagement. India has the opportunity to lead by example, crafting a framework that upholds national interests while contributing to the global digital economy.

POLICY RECOMMENDATIONS

In order for India to rapidly grow its digital economy, it needs robust digital sovereignty policies that both secure data and foster global collaboration.

India could benefit from adopting flexible frameworks like the EU's GDPR, which would ensure both stringent data protection and the free flow of non-sensitive data. India's Digital Personal Data Protection Bill, 2023, should continue to evolve by aligning with global frameworks while considering local priorities. The National Cybersecurity Policy (2021) can be upgraded to include more specific measures for critical infrastructure sectors and a stronger emphasis on preventing cyber-attacks and mitigating their impact[33]. The government could work with private tech companies, fintech firms, and digital platforms to develop industry-wide standards on encryption, compliance with data protection laws, and data sharing. Joint initiatives and collaboration between academia, industry, and government can help in creating advanced tools and technologies to enhance data security and privacy. Furthermore, the government could run campaigns that educate people on their rights under the DPDP Act along with how to exercise those rights. Public awareness campaigns should also cover the ethical use of data and the implications of unauthorized data sharing. To remain at the forefront, India could support research and development in cybersecurity technologies such as the evolving AI-driven threat detection and blockchain for secure data protection.[34]

Thus, the digital sovereignty of modern India hinges on effective policies that not only protect national interests but also encourage global connectivity simultaneously. By harmonizing domestic laws with global standards, enhancing cybersecurity, promoting public-private

[33] How Data Sovereignty and Localisation Impact Privacy Programmes (n 7)
[34] Thakur (n 1)

collaboration, and fostering digital literacy, India can succeed in developing a robust digital framework that secures India's future in the digital age.

CONCLUSION

Digital sovereignty is emerging as a defining concept in the global digital economy, and its importance is particularly critical for emerging economies like India. As digital technology evolves at an unprecedented pace, nations are grappling with the need to safeguard their national interests while ensuring seamless participation in the global digital ecosystemThe position in this regard is particularly daunting for India because, even as India continues to grow as a digital economy, cross-border data flows increasingly become important for its growth and technological development.

While India has achieved much in terms of proposing a legal framework for data protection, much remains to be achieved- particularly in relation to cross-border data exchanges and cybersecurity. The way forward would then be to craft policies that respect digital autonomy without undermining the benefits of global collaboration. Global insight could be understood on how different countries have tread their path while ensuring that it would strike a good balance between having their digital sovereignty and the unceasing global flow of data. Thus, using all this understanding India can itself build a direction through which the balance of the need for having more sovereignty to remain digitally independent also is possible. As India progresses on its path, the pursuit of digital sovereignty must be a dynamic process evolving in response to emerging trends in technology, changing landscapes globally, and the growing importance of data as a strategic resource.

India's journey to the assertion of digital sovereignty must be national and global. The challenges are substantial, but they also represent an opportunity for India to shape its future as the leader of the digital age. Crafting policies that respect nationalism and adopt internationalism, itself can bring an ecosystem of empowerment in the digital sense for Indian citizens, strengthen the economy, and play a strong role in setting the future agenda of global data governance. In this respect, it is only important to learn that digital sovereignty is not an isolation but a foundation to be able to sustain and remain inclusive in the virtual world.