DATA LOCALIZATION: AN ISSUE IN THE CROSS-BORDER DIGITAL ECONOMY

Pritam Sen, BBA LLB, CHRIST (Deemed to be University), Delhi NCR
Muskaan Chadha, BA LLB, Jamia Millia Islamia, New Delhi

ABSTRACT

The rise of data localization as a legal requirement shows how India handles digital independence against the needs of worldwide data commerce. The digital marketplace has become India's new oil because it has more than 900 million internet users, and its GDP is expected to reach $4.27 trillion by 2025, which raises worries about privacy and cybersecurity and state control. The demand for local data storage and processing comes from the requirement to safeguard personal information and stop foreign spying activities, and maintain national security. The Indian data protection system has evolved through different stages, which started with strict rules for data localization before moving toward more adaptable approaches. The B.N. Srikrishna Committee Report (2018) started the legislative process through its recommendation to define personal data and sensitive data, and critical data. The Digital Personal Data Protection Act (DPDP), 2023, now embodies a "soft localization" approach, permitting cross-border transfers under government regulation rather than imposing outright restrictions. However, this flexibility introduces challenges relating to high infrastructure costs, regulatory ambiguity, lack of international enforcement mechanisms, and cybersecurity vulnerabilities. The absence of comprehensive Mutual Legal Assistance Treaties (MLATs) further limits India's ability to access and control data stored abroad. In comparison, international experiences demonstrate wide variations. China and Russia rely on absolute data localization to protect national interests, while the EU's General Data Protection Regulation (GDPR) provides a conditional regulatory measure through adequacy decisions, consent, and contractual clauses. Compared to these international standards, India's law has gaps defined by vague definitions and restricted institutional independence, and broad exemptions for the government that weaken individuals' privacy. Addressing the problem more sustainably requires establishing specific data classifications and creating independent monitoring systems and enforcing breach reporting deadlines, and developing international partnerships. Data localization in India needs to evolve past protectionism because it requires a rights-based system that supports innovation through international standards while protecting domestic security interests.

Keywords: Data Localization, Cross-Border Data Transfers, National Security, Regulatory Challenges, Privacy and Cybersecurity

INTRODUCTION

India is catapulting itself into the digital and modern world. With over 1.46 billion, India's growth right now is enormous.[1] As of 2025, India is projected to be the fifth-largest economy, with a nominal GDP of $4.27 trillion, according to Forbes India.[2] It's looking to be a super big player in trading around the world, right there behind the United States and China. With the internet and online services penetrating, millions of people are going to international websites every single month, fueling the cross-border digital economy. Tech giants and e-commerce platforms are heavily dependent on user data from India. For instance, Facebook (now Meta) generated $117.93 billion in revenue in 2021, with 97.5% coming from advertising, largely fueled by its vast user base and increasing ad prices.[3]

The digital advancement of India creates an immediate requirement to strengthen data privacy protections and cybersecurity measures, and national security defenses. The growth of digital services has brought with it issues of data control, ownership, and security. The concept of Data localization emerged as a policy that forces organizations to keep their data within their country's borders for storage and processing purposes. The system works to prevent foreign espionage activities while strengthening cybersecurity measures and ensuring legal compliance, and protecting personal data. Localizing data storage facilities for a country like India, where data is perceived as 'the new oil', is a strategically guided action rather than sheer business foresight. Nations all over are beginning to understand the geostrategic significance of data and are enforcing strict policies concerning the spatial bounds of data flows. In India, the drive towards data localization has been multifaceted - shaped by laws as well as economic policies. In 2018, the Reserve Bank of India instituted harsh data storage policies for the financial sector.[4] Reliance, Jio, and Gautam Adani have come to acknowledge the economic and security benefits of data localization, and so are setting up domestic data centers to improve

[1] Macrotrends, *India Population Growth Rate 1950–2024*, *Macrotrends* (Apr. 2, 2025), https://www.macrotrends.net/global-metrics/countries/IND/india/population-growth-rate
[2] *"India's GDP Doubles to $4.2 Trillion Over the Past Decade: IMF," The Economic Times* (Mar. 26, 2025, 11:58 IST), https://economictimes.indiatimes.com/news/economy/indicators/indias-gdp-doubled-to-4-2-trillion-over-last-ten-years-imf/articleshow/119516457.cms
[3] CompaniesMarketCap, *Facebook Revenue 2010–2023*, *CompaniesMarketCap* (Apr. 2, 2025), https://companiesmarketcap.com/facebook/revenue/
[4] Reserve Bank of India, *Report on Trend and Progress of Banking in India 2018–19*, *Reserve Bank of India* (Dec. 24, 2019), https://www.rbi.org.in/Scripts/PublicationsView.aspx?id=19364

digital sovereignty, improve the IT infrastructure of India, provide job opportunities, and bring in foreign investment.[5] Data localization brings advantages but also compliance costs and trade barriers, which can complicate operations for multinational enterprises. With data localization, India adds another layer to its quest to become a digital sovereign, as it learns to balance the tension between digital sovereignty and global data flow, forging the future of cybersecurity, digital governance, and international trade collaborations.

CONTROVERSY

Perspective on data localization is divided among industry leaders, policymakers, and businesses. Mukesh Ambani, Chairman of Reliance Industries, one of the brightest and most vocal proponents of strict data localization, has urged Prime Minister Narendra Modi to respond to what he calls "data colonization," arguing that Indian data should be owned and controlled by Indians, not foreign tech giants.[6] Such localization would bolster data security, reduce foreign spying, and spur economic growth, according to Ambani.

Indian lawmakers have focused on soft data localization, which allows cross-border data transfer as long as certain conditions are met, instead of requiring data to be stored entirely within the borders. The Personal Data Protection Act (2018), which later morphed into the Digital Personal Data Protection Act, 2023, played a pivotal role in guiding Indian data policies, moving toward a desired flexibility of regulation. Critics say hard localization would mean inefficiencies, overlaps, and delays of services.

The business sector, including startups, fears border restrictions on data flow because they believe these rules will block innovation and stop them from reaching worldwide resources and high-tech infrastructure. Foreign companies have voiced their worries about rising expenses together with regulatory challenges, because localization rules prevent them from fully using data monetization and conducting their worldwide business operations. Foreign investors continue to hesitate about building data centers in India because they think localization requirements will decrease their profit chances.

[5] *Today on The CapTable: How Adani and Reliance Have Emerged as Data Centre Kingmakers*, YourStory (June 26, 2024), https://yourstory.com/2024/06/ambani-adani-data-centre-reliance-big-tech
[6] *Mukesh Ambani urges PM to take steps against data colonisation*, The Economic Times https://economictimes.indiatimes.com/tech/ites/mukesh-ambani-urges-pm-to-take-steps-against-data-colonisation/articleshow/67585615.cms?from=mdr

ANALYSIS OF IMPLEMENTATION ISSUES

India does not have a comprehensive data localization law in place, which raises challenges for businesses, regulatory bodies, and consumers. The main concerns include the high cost and infrastructure setup.[7] Infrastructure investment is required to build several of these local centers, potentially hindering international companies and startups and inflating operational expenses. In addition to this, there are gaps in India's digital infrastructure that will challenge efforts to implement a wide-scale data localization effectively.

The problem is exacerbated by regulatory and compliance requirements. India's evolving data policies also conflict with international laws due to the lack of uniform global standards. The lack of government notifications leaves an unregulated space. Without clear mandates, companies may continue storing data abroad, raising concerns over privacy, security, and enforcement. The internet faces a major threat from splinternet because different countries create their own data protection rules, which leads to inefficient systems and restricted access to worldwide data services. The practice of storing data within India does not prevent encryption keys from being located outside national borders, which restricts law enforcement agencies from obtaining access. The implementation of data localization practices also creates cybersecurity risks because it stops important threat data from moving between countries, which helps fight cyber threats worldwide. The absence of Mutual Legal Assistance Treaties (MLATs) between India and other nations creates barriers to accessing data for security and legal purposes.

Furthermore, data localization could inadvertently compromise cybersecurity by limiting the flow of important "threat data" required to counter cyber threats across the world. Further, the lack of Mutual Legal Assistance Treaties (MLATs) with many countries impedes India's access to data for security and legal processes.

The practice of localization provides organizations with increased control over their data, but it creates higher expenses for both consumers and businesses, which might reduce service quality and access. Most countries have stopped requiring strict localization rules in their trade agreements because they seek a middle ground between protecting national security and

[7] Aditya Gupta, *Data Localization in India: Regulations, Impact, and the Future*, (Sept. 24, 2024), https://www.metalegal.in/post/data-localization-in-india-regulations-impact-and-the-future

promoting innovation and economic growth.

STATISTICAL DATA

1. India's Digital Economy and Cross-Border Data Flows

India, with more than 900 million users of the internet, is the second-largest market online after China, reports Statista.[8] The rapid growth of Internet users in India is primarily the result of a stronger economy, greater accessibility and affordability to the internet, as well as efforts by the government like Digital India. Most internet users prefer content in regional languages, and there is a growing demand for digital services within those languages and for digital services that target local consumers. However, a significant proportion of India's data is supposedly stored on foreign servers outside of India.[9] This creates major issues regarding data privacy and data security, as that data is subject to foreign jurisdiction and laws.

2. Data Localization Costs and Infrastructure Challenges

The Indian data localization landscape is evolving, with investments projected to reach $5 billion annually by 2025, as per NASSCOM reports.[10] However, data localization measures significantly impact operational expenses, with findings from an OECD-WTO business questionnaire indicating a rise in data management costs by 15–55%.[11] A major hurdle remains the limited availability of Tier 4 data centers, essential for high-reliability applications, which forces businesses to rely on foreign cloud services.

3. Cybersecurity and Data Breaches in India

As per the Threat Landscape Report 2024 by CloudSEK, India emerged as the second-highest

[8] Priyanka Das, *Top 10 Countries With The Most Expensive Internet In 2025 (And How India Compares)*, (Oct. 10, 2025), https://www.news18.com/photogallery/tech/top-10-countries-with-the-most-expensive-internet-in-2025-and-how-india-compares-ws-el-9626443.html

[9] FE Business, *As India goes digital, experts raise alarms over sensitive data stored on foreign servers*, The Financial Express (Aug. 6, 2025), https://www.financialexpress.com/business/digital-transformation/as-india-goes-digital-experts-raise-alarms-over-sensitive-data-stored-on-foreign-servers/3938280/

[10] NASSCOM, *India: The Next Data Center Hub* (2025), *NASSCOM*, https://www.nasscom.in/knowledge-center/publications/india-next-datacenter-hub

[11] OECD & WTO, *Digital Trade and Data Flows: The Role of Data Flows for Trade in Asia* 21 (2022), https://www.google.com/url?sa=i&source=web&rct=j&url=https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/11/the-nature-evolution-and-potential-implications-of-data-localisation-measures_249df37e/179f718a-en.pdf&ved=2ahUKEwiQ9tbWs6SQAxUezjgGHeFlJDgQ1fkOegQIDRAG&opi=89978449&cd&psig=AOvVaw2OXgTzuEP7nKpQ9g6y1nuq&ust=1760555827010000

target of cyberattacks globally in the year 2024, with 95 entities being attacked.[12] On average, the cost per incident of data breach in India, as per the RBI cybersecurity report, was approximately $2.18 million, which has increased by 28% since 2020. Of these incidents, many were categorized as unauthorized network scanning and probing, indicating an urgent need for robust cybersecurity in India.[13]

LEGAL PROVISIONS

The law on data localization in India has changed quite a bit, with landmark legislations and case laws defining the policy debate. The idea emerged from the B.N. Srikrishna Committee's report on "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians," which was established by the Ministry of Electronics and Information Technology, ushering in the Personal Data Protection Bill, 2019.[14] The Committee's draft clearly identifies how data will be classified into buckets of personal data, sensitive data, and critical data, with separate localization requirements for each. It claimed that localization would improve enforcement abilities, lower risks related to data moving over global fiber-optic networks, develop an indigenous AI ecosystem, and defend against foreign surveillance. The justifications were conceptualized as national security, economic development, and digital sovereignty.

The foundation was laid, and with the Digital Personal Data Protection Act (DPDP), 2023, we witnessed a paradigm shift. Contrary to its predecessor, the DPDP Act does not mandate strict data localization but permits selective restrictions of cross-border data flows. Section 16(1) empowers the Central Government to publish a notification designating certain countries or territories where transferring personal data would be impermissible. Section 16(2) guarantees that if other Indian laws provide greater protection or limitations, then they will be the overriding factor.[15] The Act, thus, takes a pragmatic and strategic approach by balancing global data flow with sovereign interests.

---

[12] *India Ranked Second in Global Cyber Attack Targets: Report*, *Times of India* (Apr. 7, 2025), https://timesofindia.indiatimes.com/india/india-ranked-second-in-global-cyber-attack-targets-report/articleshow/116893292.cms

[13] *India's Average Data Breach Costs Hit $2.18 Mn in 2023, Up 28% Since 2020*, Business Standard (Jul. 29, 2024), https://www.business-standard.com/finance/news/india-s-average-data-breach-costs-hit-2-18-mn-in-2023-up-28-since-2020-124072900750_1.html

[14] Committee of Experts Under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Ministry of Electronics & Information Technology 2018).

[15] Digital Personal Data Protection Act, No. 22 of 2023, §§ 16(1), 16(2)

The Act also provides for exceptions under section 17, including public order, national security, and research to ensure that the scope of the Act is not broad as to override fundamental governance or R&D endeavors. At the same time, Section 8 creates vital responsibility-based obligations upon data fiduciaries, like ensuring accuracy of the data they gather, using sufficient security safeguards, and engaging processors under lawful contracts, which makes way for accountability.[16] The Act further introduces a whitelist-blacklist model for cross-border data sharing. Data can be transferred globally except to blacklisted countries, which are restricted via government notification. However, draft rules introduce complexity by imposing conditions on data flows. For example, Significant Data Fiduciaries that deal in large-scale data are subject to tighter controls, particularly on cross-border flows and personal data. Under Rule 22, the Ministry of Electronics and Information Technology (MeitY) has the power to call for additional information for designating entities as SDFs. The absence of defined criteria and regulatory gray areas makes it difficult to comply with.[17]

Section 67C of the Information Technology Act of 2000 requires intermediaries to keep certain data for specific time periods and formats as determined by the government. The regulations specify that non-compliance leads to a penalty of 25 lakh rupees. The IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, require that sensitive data transfers outside India can only happen if the foreign country provides equivalent data protection standards. In addition, the IT Intermediary Guidelines and Digital Media Ethics Code Rules 2021 require intermediaries to hand over user-related data to relevant authorities upon official request, which poses challenges when data is stored out of the country.[18]

In many landmark judgments, vigorous data protection has been demanded. In Justice K.S. Puttaswamy (Retd.) v. Union of India, pretty much all across 2017, the Supreme Court declared that the right to privacy would be fundamental under Article 21 and that any infringement would have to meet the tests of necessity, proportionality, and legality-these principles currently complete the structure of data legislation.[19]

[16] Digital Personal Data Protection Act, No. 22 of 2023, §§ 8, 17
[17] Digital Personal Data Protection Rules, 2025, r. 22
[18] Information Technology Act, No. 21 of 2000, § 67C (India); Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (India); Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).
[19] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1

In Google India Pvt. Ltd. v. Visakha Industries (2020) it was held that intermediaries must conform their conduct to Indian law and could incur liability for unlawful content if they fail to act upon notice.[20] Similarly, in the WhatsApp Privacy Policy Case (2021), the Court focused on the question of user consent and transparency in their data processing.[21]

INTERNATIONAL LAWS

Data localization laws vary greatly across jurisdictions and reflect national priorities on national security, privacy, and digital sovereignty. China has one of the strictest localization regimes, requiring, under Article 37 of the Cybersecurity Law (2017), that Critical Information Infrastructure (CII) operators keep domestic servers that store all personal data and so-called "important" data collected in China. The requirements cover areas like public communication, finance, energy, and government, with cross-border transfers permitted only following a rigorous security assessment.[22] In a similar, if slightly relaxed, way, Indonesia's Electronic Information and Transactions (EIT) Law establishes unconditional localization for general public sector data, mandating that system providers conducting operations in the public sector establish data centers in the country.[23]

Russia implements a mirroring localization model via Federal Law No. 242-FZ. All personal data of Russian citizens must be stored in Russia, and while data can be transferred abroad, a local copy must remain in Russia.[24] Under the My Health Records Act 2012 (amended 2018), Australia implements a sector-specific localization model, demanding that sensitive health data be stored within its national borders to ensure greater patient privacy.[25]

In the U.S., national security concerns drive data localization. Under DFARS Case 2013-D018, contractors who receive sensitive defense information are required to make sure that data stays within U.S. jurisdictions.[26]

[20] Google India Pvt. Ltd. v. Visakha Indus., (2020) 4 S.C.C. 162
[21] Karmanya Singh Sareen v. Union of India, Writ Petition (Civil) No. 313 of 2016 (Del. H.C. 2021)
[22] Cybersecurity Law of the People's Republic of China, art. 37 (2017)
[23] Electronic Information and Transactions Law, No. 11 of 2008
[24] Federal Law No. 242-FZ on Personal Data
[25] My Health Records Act 2012 (Cth) (Austl.), as amended by My Health Records Amendment (Strengthening Privacy) Act 2018
[26] Defense Federal Acquisition Regulation Supplement (DFARS) Case 2013-D018, "Network Penetration Reporting and Contracting for Cloud Services," U.S. Dep't of Def. (2016)

Through its General Data Protection Regulation (GDPR), the European Union eliminates the necessity of data localization but imposes tough restrictions on transferring data across borders. Data transfers to countries outside the European Economic Area (EEA) are only permitted when those countries have appropriate levels of protection or in place adequate safeguards such as Standard Contractual Clauses (SCCs) and Binding Corporate Rules. To circumvent these difficulties, most companies store data inside the EEA, thereby achieving de facto localization.[27] It enhances the protection of EU individuals' personal data, applies to data stored outside the EU, and strengthens the free movement of non-personal data within the EU. It strikes a fair balance between privacy rights and cross-border data flows.

PLUGGING LOOPHOLES

India's recent Digital Personal Data Protection (DPDP) Act, 2023, is a huge leap towards protecting data privacy; it still lags behind global standards such as the European Union's General Data Protection Regulation (GDPR). One huge loophole is the absence of unambiguous definitions of crucial terms like "sensitive personal data" and "critical personal data." This vagueness grants the government too much discretionary power; by contrast, the GDPR offers specific and well-defined categories of data.

Another shortcoming is within the self-governance and jurisdiction of the enforcement entity. The DPDP Act does make provisions for the Data Protection Board, but its autonomy is doubtful on account of its administrative affiliation with the central government. On the other hand, the GDPR provides for independent supervisory authorities that are equipped with commanding powers to enforce the regulation. Moreover, the Indian legislation does not provide for strict timeframes to notify breaches. The organization is required by the GDPR to report a data breach within three days. This guarantees accountability as well as swift response, but the DPDP Act does not specify any timelines.

Also, the Act's broad exemptions for government agencies on grounds like "national security" or "public order" raise concerns about potential misuse and lack of oversight. On the other hand, GDPR is different because it pushes for using proportionality and necessity even for things of high national importance or state secrets. And lastly, India is very weak when it comes

[27] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119/1 (General Data Protection Regulation or GDPR).

to being part of global stuff like Mutual Legal Assistance Treaties (MLATs), which are agreements so that countries can work together to help one another fight crime and share data internationally. It really makes cross-country cooperation very weak in regulating things like cybercrime.

WAY FORWARD

India must strengthen its data protection system to make it compliant with the best practices of the world. Reforms at the highest level are actually imperative for this. Firstly, the act must give proper definitions to critical and sensitive personal information so there is no ambiguity, and they can be uniformly applied. From the GDPR, India needs to implement tiered levels of protection depending on the nature of data. Second, the Data Protection Board must actually be an independent institution with legal authority so that the oversight is fully objective and people trust it. Thirdly, the law ought to require prompt breach notifications, preferably within 72 hours, to promote transparency and facilitate speedy response mechanisms. Unbridled authority in the cause of national interest that could lead to misuse, the sweeping exemptions accorded to government departments have to be limited and equipped with robust judicial or parliamentary oversight. It is also necessary to promote international relations. India needs to join international data transfer treaties and strengthen MLAT arrangements for available data, privacy, and cybercrime enforcement. To ensure complete law enforcement, awareness, and digital literacy among corporate houses, data custodians, and society in general is necessary. Certainly, the foundations of law enforcement success involve designing sensitization campaigns and training programs for private individuals and firms. India must ensure that its data governance policies are transparent but innovative, rights-based, and protective of data privacy at the individual level.

CONCLUSION

In India's quickly growing digital economy, data localization has become a sensitive and controversial issue, balancing national interests with globalized digital trade. The increasing demand for storing and processing citizens' data within national borders reflects legitimate concerns regarding privacy, cybersecurity, and legal accountability. While there is some progressive impetus, such as with the Digital Personal Data Protection Act, 2023, this will need to be digested alongside international measures, which should be fully taken into

consideration. The law suffers from vague definitions, a lack of stringency in its enforcement mechanisms, and broad discretionary powers that undermine its effectiveness.

India has been making progress in multiple sectoral regulatory and legal frameworks; it desperately needs cohesive, clear, and consistent data governance that is comparable to global know-how. A balance needs to be struck between protecting citizens' privacy and allowing a thriving digital economy to flourish. There is a need for better classification of data types, independent oversight bodies, clearer data transfer protocols , and public awareness. In an increasingly interconnected world, with an eye on the future, the Indian State's policy cannot afford to overestimate threats to sovereignty and security at the cost of individual rights and freedoms, to ensure a digital ecosystem that is conducive and participatory, along with the need for social and technological trust globally.