The Evolution of Data Localization Laws: A Cross-Country Comparative Analysis

Deep Vora

Kautilya School of Public Policy, GITAM (Deemed To Be University)

Course: Reforming the Indian Economy

Course Faculty: Dr. Amrendra Pandey

November 7, 2023

Introduction:

Data localization is the practice of requiring data to be stored or processed within a specific jurisdiction, often for reasons of data sovereignty, national security, or privacy.

- International Association of Privacy Professionals

Data is often described as the new oil of the 21st century, as it has become a key resource and asset for economic development and social progress. However, unlike oil, data is not bound by physical constraints or borders, as it can be easily transferred and processed across different countries and regions through the internet and cloud services. In the year 2021, 64.2 zettabytes of data was generated which is 314% increase from 2015, this trends shows that data is growing exponentially (United Nations, 2023). This creates various opportunities and challenges for data governance, such as how to ensure the privacy and security of data subjects, how to support the growth and innovation of data-intensive businesses, and how to respect the sovereignty and autonomy of data-producing countries. Data localization is one of the approaches to address these issues, as it directs that data must be stored and processed within the jurisdiction of a specific country or region.

India is a developing nation that wants to have an economy of $5 trillion by 2025. Its digital industry has a huge potential to increase to about $1 trillion. Additionally, India is a major exporter of digital services, after USA and Canada being top two markets for exports. In the year 2020, it estimated that 1% rise in digital service exports results in a 0.02 % boost in India's GDP (CUTS International, 2020, p. 42). India's exports of digital services depend on favourable regulations abroad that provide open market access, including the capability of cross-border data transfer. However, India also has to deal with issues like foreign surveillance, lost economic benefits from data exploitation by foreign parties, misuse of personal data, and data storage on foreign servers, all of which obstruct domestic national

security agencies' access to data. India has several rules that mandate data localization or limit the movement of data across borders that are now in place or that have been suggested to address these challenges. These laws include the Digital Data Protection Act of 2023, the Information Technology Act and Rules of 2011, the RBI Notification on Storage of Payment System Data.

These policies seek to safeguard data subjects' privacy and security, foster local industries and innovation, improve law enforcement access to data, or establish national sovereignty over data. However, they have implications for India's digital economy, as they may increase the cost and complexity of doing business, reduce Indian firms' competitiveness and efficiency, limit access to global markets and technologies, and affect the quality and availability of digital services for Indian consumers.

The research paper will look at different policies that highlight problems with data localization in India, the effects of restricting cross-border data flow on India's export of digital services, regulatory issues, the cost and challenge of building infrastructure, privacy issues, cybersecurity, etc. The report will also do comparative analysis of different countries and its scope and impact on it.

Methodology:

The paper will examine the concept and effects of data localisation in India using Adrian Kay's *Evolutionary framework* (Peters & Fontaine, 2020, p. 385). The evolutionary framework is a thorough method for examining how policies change and adapt through time and in different situations, depending on a variety of circumstances. The paper will use *Qualitative causal case studies* as the method for analysis (Peters & Fontaine, 2020, p. 238). The paper will identify the causes, impacts, and effects of data localization on various stakeholders, such as the government, industry, civil society, and foreign entities.

Further, through evolutionary framework paper will look at the development of India's data policy, starting with the K.S. Puttaswamy decision which declared the right to privacy under Article 21 a basic freedom right (Mustafa, 2017). In addition, the RBI circular, which required all payment system providers to store data in India starting in 2018, and the various bills and notifications that suggested data localization measures for various types of data, including personal, non-personal, e-commerce, or health data, will be examined in the paper.

Through a causal case study, the paper will provide a comparative analysis between countries, like the India, European Union, Indonesia, and China that have enacted or proposed data localization laws. The analysis table will look into the scope of the law, the rationale behind bring the law and the outcome of the law pertaining to data localization in that particular country.

Evolution of Data localization in India:

In India, the emergence of data localization has been a dynamic process identified by several of significant incidents and legal changes. The issue has been a source of contention among many stakeholders, with various points of view expressed in various industries and circumstances.

The Supreme Court of India's significant decision in K.S. Puttaswamy versus Union of India in 2017 was an important turning point (Solanki, 2023). The right to privacy, including the right to informational privacy, was recognized as a basic right by the court. This decision emphasized the importance of comprehensive and up-to-date data protection regulations.

In 2018, the Reserve Bank of India took a major step towards data localization. It issued a circular mandating all payment system providers to store all data related to their payment systems solely in India. This directive sparked numerous debates and discussions

among stakeholders. The year 2019 saw the introduction of the Personal Data Protection Bill (PDBP) in Parliament. The bill, based on the recommendations of the B.N. Krishna committee, proposed a graded approach to data localization (Author et al., 2022). It categorized data into three types based on their sensitivity: personal data, sensitive personal data, and critical personal data.

However, the Digital Personal Data Protection Act of 2023 took a different approach. Instead of classifying personal data into three categories, it defined data, personal data, and digital personal data. This act marked a significant evolution in India's approach to data localization.

The proposed categorization in the previous bill had various implications. Different Stakeholders from the industry, experts, have argued about the challenges posed by both the proposed bill and the current act in defining data localization. This ongoing debate and the evolving legislation reflect the complexity of data localization in the digital age. Indeed, this can be seen as an evolution of data localization in India.

Emergence of Data Localization Laws across World:

Since the Internet became widely used in the 1990s, governments have faced many difficulties in managing and protecting the growing and diverse digital data. The rise of online piracy, malware, and data regulation issues have made it hard for governments to implement effective policies. After Edward Snowden exposed the NSA's massive online spying, data security and privacy became major concerns for the global public (Coyne, 2019). Therefore, governments are now more eager to take strong actions to safeguard their national data and privacy.

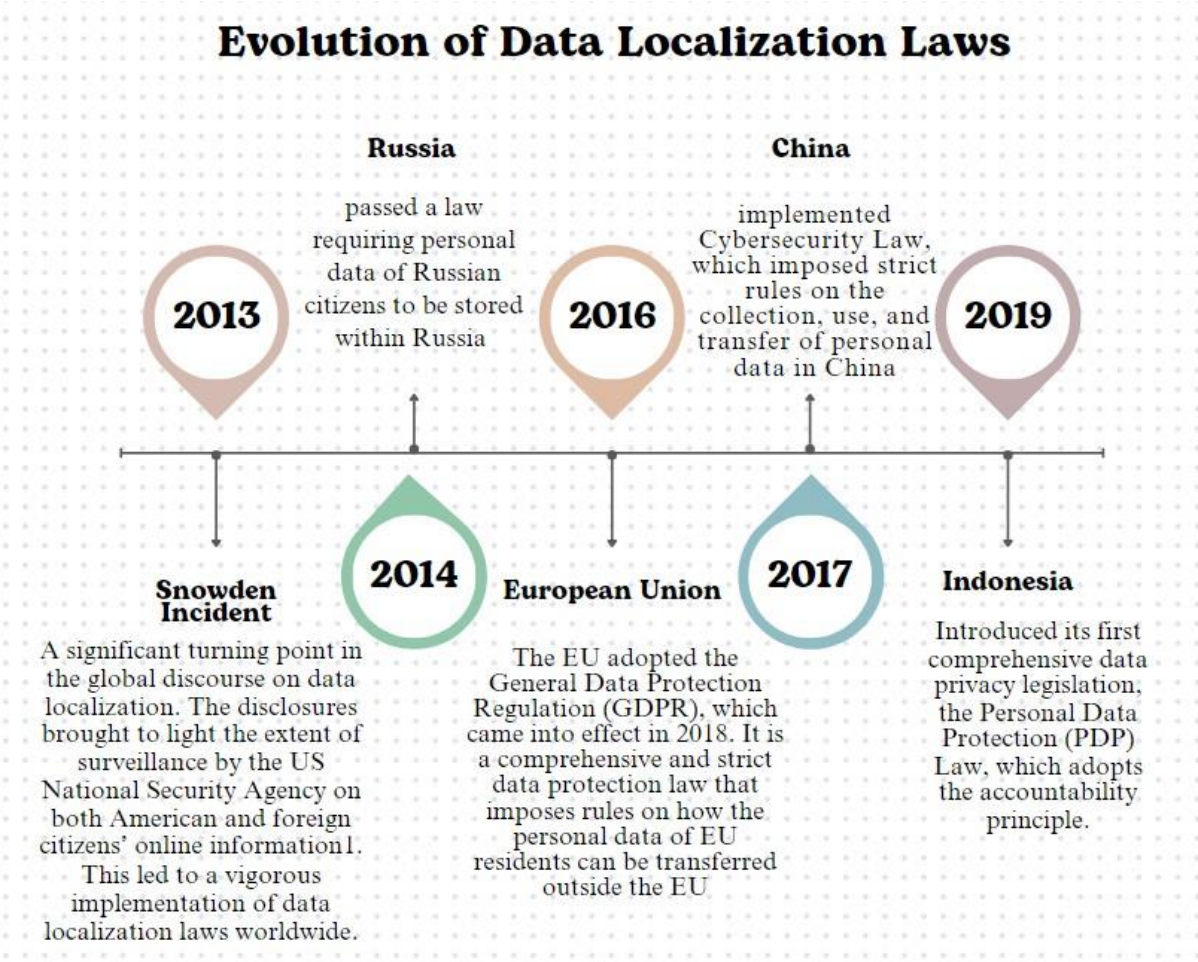
Today, more than a dozen nations, both developed and developing, have enacted or are actively considering enacting data localization legislation. The techniques and consequences of the laws, prohibitions, and policies under examination are various. Proposals

include requiring local ownership of data storage infrastructure, limiting international internet shops, and forcing local hiring. While authoritarian regimes like as Russia, China, and Iran employ data localization to control and watch its citizens, data localization laws are often seen as successful.

However, even democratic nations are taking these more expansive data localization requirements seriously. Brazil, Indonesia, and India, which have seen some of the most furious anti-NSA protests, are now considering passing massive data localization legislation.

The EU is also considering localization within its jurisdiction.

Timeline:



The Edward Snowden revelations in 2013 marked a significant turning point in the global discourse on data localization. The disclosures brought to light the extent of surveillance by the US National Security Agency on both American and foreign citizens'

online information. This led to a vigorous implementation of data localization laws worldwide.

Russia imposed stringent data localization rules in response to the Snowden revelations. According to these regulations, any foreign or Russian data operator that gathers personal information about Russian residents, including over the internet, must first use Russian databases to record, store, organise, update, and retrieve the information. This law was a reaction to both domestic and regional issues.

Similarly, in China, data related to citizens are stored, processed, and handled within China under a strict law. However, the EU's General Data Protection Regulation allows transfers of personal data to locations outside of the European Economic Area only under certain conditions. Meanwhile, Indonesia has recently enacted a law to protect data and privacy specifically for electronic systems and transactions.

Comparative Analysis of different countries:

This comparative analysis will examine the different laws of countries related to data localization and their scope, rationale, and outcome. It will explore what factors influenced the countries to adopt certain provisions in their laws and what effects they might have. The European Union law is the most comprehensive and detailed one that focuses on protecting its citizen data within the EU and allows some exceptions. China's law is the most extreme one that aims to safeguard its data from foreign interference and domination by imposing strict rules and regulations. Indonesia's law is the most recent one that regulates the data and privacy of electronic systems and transactions and tries to limit the data outflow and enhance the data sovereignty of the country (Alam & Bedekar, 2018). These laws show the different motivations and challenges of these countries in the context of data-driven economy and globalization.

Table:

One of the key issues in the global digital economy is the cross-border transfer of personal data, which is subject to different legal frameworks and regulations in different countries. The table given below compares the data protection laws of four countries: India, the European Union, China, and Indonesia, and shows how they differ in their scope, rationale, and outcome.

Country	Law	Scope	Rationale	Outcome
India	Digital Personal Data Protection Act, 2023	1. Critical personal data can only be processed within India. 2. Sensitive personal data can be transferred outside India with explicit consent and adequacy or contractual safeguards,	1. To ensure the security and integrity of critical personal data of national importance.	1. It May enhance the security of critical personal data within India, but may also hamper the free flow of data and innovation across borders. 2. May create barriers and costs for foreign companies to access the Indian market.

European Union	General Data Protection Regulation (GDPR,2018)	1. Personal data can be transferred outside the EU with consent or adequacy or appropriate safeguards. 2. Cross-border transfer of personal data is also allowed under other legal bases, such as consent, contractual performance, public interest, or legitimate interest.	1. To protect the fundamental rights and freedoms of natural persons in relation to their personal data. 2. To ensure the free movement of personal data within the EU and with third countries that ensure an adequate level of protection.	1. Enhances the protection of personal data within and outside the EU, and supports the development of the EU's digital single market and global digital economy. 2.Enhances the competitiveness of EU companies in the global digital economy.

China	Cybersecurity Law (2017) and Data Security Law (2021)	1. Personal information and important data collected and generated by critical information infrastructure operators must be stored within China. 2. Network operators must comply with the relevant standards and rules for collecting, storing, using, transferring, and deleting personal information.	1. To protect the national security and public interest of China. 2. To promote the development of China's digital economy and domestic industry	1.Boosts the competitiveness of domestic companies in the Chinese market, but restricts the access and operation of foreign companies in China. 2. Promotes innovation in the local digital ecosystem and domestic industry.

Indonesia	Personal Data Protection Law in 2019	Electronic transaction data for public and non-public services must be stored within Indonesia.	To promote the development of local data storage and processing capabilities.	May affect the competitiveness of foreign companies in the Indonesian market.

Analysis:

All four nations have certain limits on the cross-border transfer of personal data, although the degree and criteria of such restrictions vary. For example, India has the most rigorous restrictions on the transfer of critical personal data, which may only be processed within India, whereas the EU allows the transfer of personal data under several legal bases, such as consent, adequacy, or sufficient safeguards. India and the EU have comparable categories of personal data; however, their definitions and handling of each category varies. For instance, India defines sensitive personal data as including financial, health, biometric, and genetic data, while the EU defines it as including racial, ethnic, religious, and political data.

China and Indonesia have similar requirements for data localization, i.e., storing data within their own territories, but they differ in the scope and rationale of such requirements. For example, China requires data localization for personal information and important data collected and generated by critical information infrastructure operators, while Indonesia requires it for electronic transaction data for public and non-public services. China and Indonesia both aim to promote the development of local data storage and processing

capabilities, but China also cites the protection of national security and public interest as a rationale.

However, The EU has the most comprehensive and harmonized data protection law among the four countries, as it covers all aspects of data processing and applies to all member states and third countries that interact with the EU (Bahl et al., 2023). The EU's General Data Protection Regulation (GDPR) aims to protect the fundamental rights and freedoms of natural persons in relation to their personal data, and to ensure the free movement of personal data within the EU and with third countries that ensure an adequate level of protection.

The outcomes of each country's data protection law depend on various factors, such as the level of protection, the balance between security and innovation, the impact on domestic and foreign businesses, and the alignment with global standards and norms. For example, India's data protection law may enhance the security of critical personal data within India, but may also hamper the free flow of data and innovation across borders. The EU's data protection law may enhance the protection of personal data within and outside the EU, and support the development of the EU's digital single market and global digital economy.

China's data protection law may boost the competitiveness of domestic companies in the Chinese market, but restrict the access and operation of foreign companies in China. Indonesia's data protection law may affect the competitiveness of foreign companies in the Indonesian market.

Recommendations:

Data localization is a complex and controversial issue that entails various trade-offs and challenges. Here are some recommendations:

- In order to improve cross-border data flow while maintaining a standardisation approach, global leaders should concentrate on multilateral cooperation on data sharing and information access. Through the promotion of openness and the removal of trade obstacles, this strategy will assist nations in harmonising their definitions and classifications of personal data.
- Governments would be able to determine the rationale behind data localization and ensure that international norms and principles are adhered to by establishing bilateral or multilateral agreements with other countries on the grounds of supporting a standards-based approach to data exchange.
- Governments may encourage local industrial partners to invest in dependable data infrastructure. Enacting fair policies like tax breaks and funding for infrastructure development would contribute to data security.

Conclusion:

India, as a major global data generator, needs to be cognizant of the evolving data governance scene. To ensure that the rights of our people are protected, we need to look into the possibility of multilateral collaboration and the establishment of data-sharing agreements with other countries. In addition to preserving its data, this will assist India in meeting international norms and aspirations. Cross-border data transfers have grown in importance as a vital part of the global economy in the digital age. The study in the article demonstrates that different approaches to data localization are taken by nations including Indonesia, China, India, and the European Union, each with their own set of standards and goals.

However, to ensure both Indian economic competitiveness and the preservation of individual rights, it is imperative that the country's data protection laws be brought into compliance with international norms and that the development of data storage infrastructure be encouraged. International data flows will remain vital to the global economy and India's digital sector. India can establish itself as a frontrunner in the safe and ethical handling of data by fortifying its legal framework in accordance with global norms.

References

Alam, M., & Bedekar, G. (2018, November 18th). *Book template-8*. The Dialogue. Retrieved November 7, 2023, from https://thedialogue.co/wp-content/uploads/2020/01/DataGlobalisation-in-a-Globalised-World-copy_compressed.pdf

Author, G., Mathi, S., & Johari, S. (2022, December 14). *The genesis and evolution of India's data protection and privacy regime*. MediaNama. Retrieved November 7, 2023, from https://www.medianama.com/2022/12/223-genesis-evolution-india-data-protection-regimeviews/

Bahl, R., Bagai, R., & Sawhney, N. (2023, August 18). *Indian Data Protection Law versus GDPR – A Comparison*. AZB & Partners. Retrieved November 7, 2023, from https://www.azbpartners.com/bank/indian-data-protection-law-versus-gdpr-a-comparison/

Coyne, H. (2019, November 15). *The Untold Story of Edward Snowden's Impact on the GDPR*. The Cyber Defense Review. Retrieved November 7, 2023, from https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Fall%202019/CDR%20V4N2-Fall%202019_COYNE.pdf?ver=2019-11-15-104104-157

CUTS International. (2020). *Data Localisation India's Double-Edged Sword?* https://cutsccier.org/pdf/data-localisation-indias-double-edged-sword.pdf

DLA PIPER. (2019, March 9). *Data protection laws of the world*. Retrieved November 7, 2023, from https://www.dlapiperdataprotection.com/index.html?t=world-map&c=CA

Gaur, V., & Sreekumar, K. (2023, August 15). *A dawn of a new era for data protection in*

India: an in-depth analysis of the digital personal data protection act, 2023 - data Protection - India. Mondaq. Retrieved November 7, 2023, from https://www.mondaq.com/india/dataprotection/1355250/a-dawn-of-a-new-era-for-data-protection-in-india-an-in-depth-analysisof-the-digital-personal-data-protection-act-2023-

Is data localization coming to Europe? (2022, August 23). International Association of Privacy Professionals. Retrieved November 7, 2023, from https://iapp.org/news/a/is-data-localizationcoming-to-europe/

Kamdar, M. (2022, February 24). The Great India Data localization puzzle. *ET CIO*. https://cio.economictimes.indiatimes.com/news/big-data/the-great-india-data-localizationpuzzle/89787780

Mustafa, F. (2017, August 25). Right to Privacy: What the Supreme Court said. *The Indian Express*. https://indianexpress.com/article/explained/supreme-court-right-to-privacy-constitutionfreedom-of-religion-simply-put-privacy-and-more-what-sc-said-4812192/

Peters, B. G., & Fontaine, G. (2020, 04 02). Handbook of Research Methods and Applications in Comparative Policy Analysis. *Evolutionary theory in comparative policy analysis*, 385–400. https://doi.org/10.4337/9781788111195.00032

Peters, B. G., & Fontaine, G. (2020, 04 02). Handbook of Research Methods and Applications in Comparative Policy Analysis. *Causal case studies for comparative policy analysis*, 238–253. https://doi.org/10.4337/9781788111195.00022

Solanki, S. (2023, August 3). *India's privacy bill (DPDP, 2023): A Detailed Analysis*. Deepstrat. Retrieved November 7, 2023, from https://deepstrat.in/2023/08/03/indias-privacy-bill-dpdp2023-a-detailed-analysis/

United Nation. (n.d.). *Big data for sustainable development | United Nations*. the United Nations. Retrieved August 24, 2023, from https://www.un.org/en/global-issues/big-data-forsustainable-development

Viswanath, N., Suri, S., Ahmed, N., Dash, A., Vijayanambi, N., & Kanakia, R. (2023, August 11). *Faqs on the digital personal data protection act, 2023*. IndusLaw. Retrieved November 7, 2023, from https://induslaw.com/publications/pdf/alerts2023/Induslaw_FAQs_on_The_Digital_Personal_Data.pdf