Journal of Contemporary Law and Society, *Volume 1, Issue 3, September 2024, pp. 144-154*

TECHNICAL ARTICLE
Online ISSN: 3139-1079
DOI: 10.18311/JCLS/2024/v1i3/48882

Online ISSN : XXXX-XXXX

INFORMATICS JOURNALS

Journal of Contemporary Law and Society

Contents available at: *www.informaticsjournals.co.in/index.php/jcls*

JCLS

Data Localization Dilemmas: Navigating The Intersection of ASEAN's Digital Economy and Fintech

Dr. Puranjan Prasad Paul

Faculty of Law, ICFAI University, Kamalghat, Agartala – 799210, Tripura, India; puranjanpaul@iutripura.edu.in

Abstract

The uninterrupted exchange of data across borders represents a fundamental principle of the digital realm, echoing the ancient Indian cultural ethos of "Vasudeva Kutumbakam—One World One Family." The economic integration of any economy is fundamentally contingent upon the unobstructed flow of data across borders, given individuals' reliance on a diverse array of fintech applications to meet their daily requirements. The increasing inclination towards financial assistance fosters the development of a digital economy within a nation. Numerous financial technology applications require continuous and unobstructed data flow across international boundaries to ensure optimal service efficiency. Nevertheless, the flow of data across borders undermines the confidentiality of individuals, which, in turn, maintains a certain sanctity within the constraints of the constitutional framework. The nations of ASEAN have paved the way for the digital economy within their data governance frameworks through exemplary initiatives, notably the ASEAN Master Plan 2025, which highlights the significant advancement of the digital economy by 2025. The primary challenge in this regard lies in the principles of data localization, which impede the unobstructed flow of data across international boundaries. This paper aims to critically assess the international reports from the OECD and the World Economic Forum concerning data localization principles alongside pertinent research studies in this domain. This paper seeks to determine the impact of the digital economy in the ASEAN nations and the consequences of data localization principles. This paper presents a thoughtful endeavour to formulate recommendations to reconcile data localization's beneficial and detrimental facets.

Keywords: *ASEAN Countries, Data Localization, Digital Economy, Economic Integration*

1.0 Introduction

The digital economy encompasses the sector propelled by billions of daily online interactions among individuals, enterprises, devices, data, and processes. Hyper-connectivity, defined as the enhanced interconnection among individuals, organisations, and machines facilitated by the Internet, mobile technologies, and the Internet of Things (IoT), constitutes the cornerstone of the digital economy (Shi *et al.*, 2022, p.2) ASEAN possesses robust underpinnings to facilitate the long-term advancement of the digital economy, characterised by a burgeoning young and technologically adept population, escalating industry digitisation, and substantial consumer demand for e-commerce (Kim *et al.*, 2020, p.3) Significant further effort is necessary to guarantee that ASEAN achieves the anticipated $300 billion internet economy within five years, especially concerning data governance. Data has probably emerged as the most valuable asset, indispensable to public and private sectors due to its tangible, quantifiable worth and extensive applicability (Kingsbury, 2003, p.273) significant further effort is necessary to guarantee that ASEAN achieves the anticipated $300 billion internet economy within five years, especially concerning data governance. Data has probably emerged as the most valuable asset, indispensable to public and private sectors due to its tangible, quantifiable worth and extensive applicability. Leveraging global data infrastructure has facilitated cross-border economic activity, permitting firms to access previously unreachable markets. The

digitization of economies and international commerce enhances information accessibility and enables more effective market operations, ultimately improving efficiency and productivity. Over the previous decade, worldwide data flows have surged by 45%. By 2025, 463 exabytes of data are projected to be generated worldwide worldwide, surpassing 2 million DVDs produced daily (French *et al.*, 2020, p.3)

As data increasingly drives economic growth, member states must implement robust, business-friendly, and progressive data governance policies that facilitate secure cross-border data flows. This theory encompasses the crucial element of data localization, whereby ASEAN countries inhibit the unimpeded movement of data across borders. The ASEAN community actively implements data localization principles. The paramount factor necessitating enhanced data localization is personal digital data and people's financial data, as it evolves daily, contributing to the emergence of 'Big Data.' (Hartung, 2018, p. 4) Any compromise of extensive data renders millions of personal and financial information susceptible.

2. Legal Materials and Methods

Data localization and its adverse effects on the digital economy can be better understood because analyzing findings derived from secondary sources such as reports from ASEAN, OPEC, the World Economic Forum, and others is essential. The authors conducted a quantitative analysis of various credible reports, observations, and findings from highly regarded international institutions. The authors conducted a thorough assessment of the ASEAN Master Plan 2025 to examine the perspectives of the ASEAN Community about the Digital Economy in the forthcoming years. The authors evaluated the OPEC report concerning data localization principles and their implications for the digital economy.

Specific primary sources were evaluated during the research to facilitate a comparative analysis of the data localization principles prevalent in the ASEAN countries. The Chinese government is rigorously enforcing data localization principles, a decision that appears to prioritize national policy over potential impacts on the global economy.

The recently enacted legislation in India regarding data governance has been acknowledged as the country capitalizes on the swift expansion of the global digital economy. The authors have provided an overview of the regulations the Reserve Bank of India set forth, marking a significant development in the country's efforts to control financial data. The OECD produced detailed reports analyzing the effects of data localization principles on the economic growth of various countries. The author presented relevant data from primary research in these reports. To identify the specific indicators, the authors thoroughly examined these reports.

The authors have analysed various data localization principles and the potential for a digital economy in the coming years. Both published and unpublished reports, including those related to the financial economy and international organizations, were utilized as secondary sources. The writers examined working papers, articles, and polls regarding virtual space components and referenced international web sources to enhance their understanding of the topic.

3.0 Fintech: An Emerging Dependency of Individuals

The emergence of financial technology (Fintech) firms, predominantly technology-driven organizations within the financial sector, has necessitated improvements in banking processes. In the modern era defined by the digital revolution, technology has profoundly influenced all sectors, including banking through financial technology. ("Acknowledgment to the Reviewers of FinTech in 2022", 2023, p. 68) Fintech, or financial technology, is delivering financial services using digital platforms. Several start-up businesses have recently emerged in the Fintech space, providing services inside the traditional banking sectors, such as loans, payments, and personal finance. Fintech services, which include peer-to-peer lending, insurance, and mobile wallets, have entirely changed how people and businesses carry out their daily transactions. In addition to providing traditional banking services, financial technology, or fintech, it does so with exceptional speed and efficiency (Law, 2024, p. 33). With the continuous advancement of technology and the ability to innovate, organisations can extend their reach to clients and those who need to access banking institutions. Financial Fall and Financial restoration is inevitable to any country but any cross border transfer for the prosperity of economy shall required to be embedded with privacy contours (Marek, 2008, p.3).

Safeguarding individuals' data by data privacy rules and regulations is essential in digital banking. Ayaburi (2022) states that the General Data Protection Regulation (GDPR) provides individuals with specific rights regarding their data, including the right to access their data, the right to be informed about its collection and use, and the right to request its deletion. To protect personal data and comply with legal obligations, businesses must establish suitable safeguards and obtain explicit consent from individuals to process their personal information, especially in specific circumstances. (Law, 2024b, p. 21).

To stay in compliance with data protection requirements, organizations must take several precautions to prevent any possible data privacy breaches. The processes include encryption, secure authentication, de-identification, regular reviews, and data protection rules. Data governance frameworks greatly assist in promoting appropriate and ethical management of extensive data. These frameworks accomplish this by outlining the responsibilities of each party, creating standards for the proper management of data, and putting measures in place to ensure compliance. Crystal Abidin argues that it is critical to establish procedures for discovering and fixing data privacy breaches, to teach employees about data security standards, and to conduct frequent audits. (Chen *et al.*, 2023, p. 8) To mitigate confounding bias and unauthorised access to personal data, it is imperative to employ meticulous data analysis and privacy-preserving machine-learning techniques while utilising Artificial Intelligence systems. Without artificial intelligence technology, the intermediate is responsible for appropriately processing the input. The intermediaries are responsible for preserving and retaining information, which may also include adherence to standards for data security and privacy; they carry the obligation of implementing "reasonable security practices and procedures." In India, intermediaries are classified as "body corporate" per section 43A Explanation (i) of the Information Technology Act, 2000.

Furthermore, section 43A of the Act explicitly states that a corporate entity that possesses, manages, or processes sensitive personal data or information within a computer resource it owns, controls, or operates and is negligent in enforcing and upholding reasonable security practices and procedures, resulting in wrongful loss or gain to any individual, shall be liable to compensate that individual for damages. (Abidin, 2020, p. 101).

Intermediaries must retain information while implementing and maintaining appropriate security practices and procedures. Failure to comply with these provisions may lead to criminal and civil liability, as outlined in sections 67C and 43A. Rule 3(4) of the Information Technology (Intermediaries Guidelines) Rules, 2011, mandates preserving information and related records for ninety days for investigative purposes. The intermediary should establish a due diligence framework that may serve as a civil or criminal litigation defence, especially in light of sections 79 and 80 of the Information Technology Act, 2000.

4.0 Financial Data: Important Facets of the Digital Economy

Harold Lasswell's foundational work on politics, released in 1936, scrutinizes the traditional methods of political study and highlights the importance of knowledge as an essential asset in the execution of 'statecraft.' The text the user provides requires expansion to be reformulated in an academic style. The governance structure of modern societies is based on the processes of acquiring, sharing, and applying knowledge (Soni, 2020b, p. 220) To adeptly oversee and navigate a large populace's complex economic and social interactions, sovereign entities must obtain extensive information regarding their citizens. Acquiring, categorizing, organizing, and analyzing large volumes of data is fundamental to a comprehensive understanding of political economy. The administration grounded in data represents the dominant expression and implementation of authority within modern society's political, social, and economic spheres.

The preservation of financial records is of paramount significance within law enforcement protocols. The execution of welfare policies is profoundly contingent upon the government's ability to engage with financial databases and records that encompass the transactions of both individuals and corporations. The data about financial transactions is of significant importance to law enforcement agencies. Financial transactions possess the capacity to uncover tax evasion, money laundering, and the financing of terrorism. By analysing supplementary personal information, one can infer sexual orientation, health status, religious and political beliefs, and cultural inclinations based on behaviours, transactions, and spatial movements.

Financial transparency and securitization became regulatory priorities after the 2008 financial crisis and the 9/11 terrorist attack. European legislation modifications have increased fund transfer and storage customer identification, record-keeping, and data retention requirements. Offshore financial centres' wealth evading national fiscal laws is likewise prohibited. Even fiscal havens lost financial secrecy. ("Financial Crisis, Financial Control", 2018, p. 11) The capillarity of public-private informational networks, which differ by area and industry, dictates the implementation of these policy objectives. Moreover, European regulators have emphasized privacy to improve the trustworthiness of influential intermediaries. The GDPR enhances efforts to provide individuals with specific legal rights over their data which commercial entities that gather such data for business purposes must ensure (Kuner, 2023, p. 101)

The post-COVID period has seen a notable increase in demands for greater transparency, enhanced documentation practices, and intensified oversight of financial information channels. These demands are motivated by the necessity to maintain the principles of due process, justice, and equality. It is essential to define specific boundaries for pursuing efficiency improvements, considering the potential impact on privacy and fundamental rights. (Belova, 2021, p. 89). Analyzing surveillance-driven enforcement networks focused on financial databases requires a thorough assessment of their extent and commonality and examining the stakeholders involved in their creation and maintenance. The significant reliance on private intermediaries raises questions regarding the reliability of these entities in executing their enforcement responsibilities (Kienscherf, 2022, p. 25) The events of 2008 showed that private organizations' self-interested pursuits do not always align with the general welfare of society. The system's over-reliance on financial firms to control risk led to its downfall. The same is true if financial organisations are tasked with protecting people's privacy and well-being, which could have regrettable results.

5.0 Digital Economy Interplay with Data Localization

Financial institutions are subject to the same economic motivations that affect data practices in other sectors. The value of data depends on its accessibility to others, specifically, the capacity to derive similar insights from it. For example, using a game-theoretic framework, it is observed that the value of consumer data may significantly decrease (potentially to zero in theoretical models) when other firms gain access to it, resulting in non-exclusivity of the data. After data generation, often facilitated by a service exchange, consumers are inclined to share this data with another company, even for a nominal fee, since sharing does not involve opportunity costs. (Carbonell- Nicolau, 2024, p. 58) The outcome mentioned arises directly from the characteristic of data being non-rivalrous. This implies that enterprises will ultimately possess identical datasets in a scenario where data exchange is seamless and incurs no transaction costs for consumers. The prospective purchaser of this data is solely interested in obtaining it on a single occasion, as each dataset is considered an ideal replacement for the others. This implies that companies participate in intense pricing competition when selling the data, commonly referred to as Bertrand competition (Dugar & Mitra, 2016, p. 1644). In due course, they compete until they reach minimal costs, resulting in the sale of data at a price that approaches zero. If a single corporation had sole possession of the data, it would have been able to demand a fee that is not zero. In this context, while data utilisation is not subject to rivalry, there is ongoing debate on the economic value that may be extracted from data.

If interpreted literally, this argument presents a compelling rationale for refraining from data sharing, as it would initially undermine the motivation to gather data. The modern global economy depends heavily on data movement across international borders. It allows businesses to trade and conduct business internationally while giving consumers access to the world's markets for goods and services. (Collignon, 2012, p. 164) The Internet's ability to function as an unrivalled source of knowledge and a means of communication that helps people in both wealthy and developing nations is also dependent on the free flow of data across national boundaries. The Internet The economy, becoming increasingly important to Southeast Asia, relies on unrestricted data flow across international borders. The ability to move data across borders has become increasingly crucial to sectors outside the Internet economy. With this ability, businesses can access, among other things, cloud computing, data analytics, and payroll management from foreign service providers.

Data localization has made it more difficult for data to transit across international borders. Data localization is the term used to describe the occurrence where a nation forces data to remain on its soil.

Data localization is primarily accomplished by countries restricting entities that own or control data. (Permana, 2019, p. 27) Data localization regulations have been found to impose costs and inefficiencies throughout the economy, which have yet to be comprehensively quantified or widely deliberated upon. The impact is most pronounced in regions where future growth and opportunities are concentrated, such as digital trade, e-commerce, global value chains, digital services, and fintech innovation. Data localization pertains to a specific aspect of the evolving environment, wherein several interconnected factors are progressing simultaneously but independently inside distinct industries and sectors. These factors are governed by regulations initially designed for a world primarily focused on tangible products and non-digital services. The current frameworks need to demonstrate more in addressing the needs of the digital economy. It is imperative to do a more comprehensive analysis of the complete expenses associated with data localization policies. This is necessary to reconsider the current trajectory of this rapidly advancing and widespread policy trend that may mitigate the potential negative impacts on global productivity, economic growth, and the equitable distribution of opportunities and it should be considered a top priority for the international community.

Data localization regulations impede the flow of data across borders. Data Localization and the ASEAN Economic Community forbid data controllers from moving data outside the territory or compelling data controllers to take specific actions on data inside the region. The need for data localization is frequently justified by national interests. Data localization, however, poses a significant risk since it prevents the exchange of services and, more broadly, acts as a barrier to economic integration. There has also been a lot written in the (mostly negative) academic commentary on the potential drawbacks of data localization, such as harming data security, increasing business costs, impeding the growth of specific industries, facilitating government surveillance and oppression, and endangering the operation of the Internet.

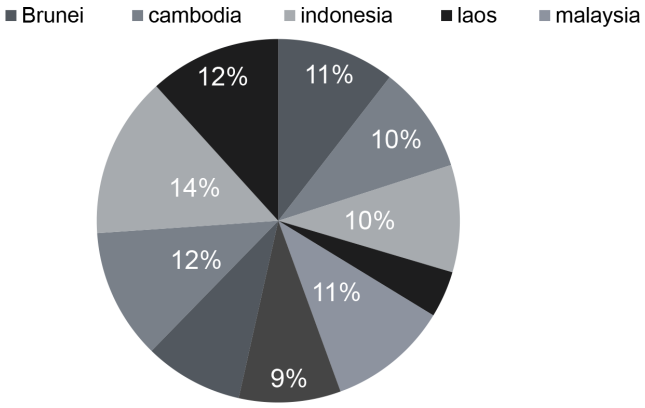


Figure 1. Distribution of Internet Market Across ASEAN Counties.

As more nations enforce regulations requiring data to be preserved within their borders, the need for data localization has multiplied globally. China's Cybersecurity Law mandates that operators of China's crucial information infrastructure who collect or produce personal or significant data must store the data within China, a prominent recent example of data localization in Asia (Permana, 2019, p. 30) The new legislation namely Digital Personal Data Protection Act, 2023 envisage that the Indian government has published aims to limit the cross-border transfer of personal data outside of India and incorporates a need for data fiduciaries to maintain at least one copy of their client's data within India. (Fraser, 2016, p. 368)

These data localization rules are frequently justified but could impede regional economic integration. Given this danger, a logical, predictable, and rules-based approach to data localization is required. In this context, the Association of Southeast Asian Nations would work effectively as a base for ASEAN Member States to create a coordinated strategy for data localization.

Figure 1 herein depicts the gradual increase of data localization principles over the years. This figure 1 is pertinent in the present research paper's pretext because most countries adopt the data localization principles based on Storage, Free Flow of data, Cross and border Data. The Figure 1 clearly states the inclination of digitalisation of every ASEAN country that perhaps tranquil the digital economy of the ASEAN Community As a result, there is an impact on the digital economy and the nation's growing economy.

6.0 ASEAN Internet Market: A Booming Digital Economy

The Association of Southeast Asian Nations (ASEAN) has emerged as the most rapidly expanding Internet market

globally. The ASEAN digital economy is anticipated to experience substantial growth, with a predicted increase of over 125,000 new users joining the Internet daily. This growth is expected to contribute significantly to the regional GDP, with an estimated addition of US$1 trillion over the next decade. The chart below addresses the percentage of smartphone users in the ASEAN Countries that eventually form significant personal and financial data across the spectrum.

However, numerous substantial obstacles hinder the actualisation of this potential. Based on the Global Digitisation Index, which assesses a nation's capacity to leverage the advantages of the digital economy, Southeast Asian countries exhibit diverse levels of progress in their developmental trajectories. Among the 100 polled countries, Singapore secured the seventh position, while Malaysia attained the 29th. However, Indonesia, Thailand, and the Philippines could not confirm a place among the top 50. The discrepancy can be attributed to the inadequate and unreliable telecommunications infrastructure in rural regions of Southeast Asia, hence impeding the potential for digital-driven development.

ASEAN has implemented significant legislative initiatives and frameworks, such as the AEC Blueprint 2025, Masterplan on ASEAN Connectivity 2025, and the e-ASEAN Framework Agreement, to tackle these obstacles and promote fair competition. The following table presents an overview of the diverse initiatives the Association of Southeast Asian Nations (ASEAN) has formulated to address the digital divide within the region.

7.0 Data Localization in ASEAN Countries: A Comparative Analysis

The Asian region lacks consensus on data localization regulations, resulting in a lack of regional peace. Navigating the regulatory landscape can pose challenges, particularly in areas subject to law, such as telecommunications, finance, and insurance. Various data localization regulations exist in the Asian region. These requirements may apply to sensitive or critical personal data and are established within the privacy legislation framework. In the case of China, these requirements extend to both critical and personal data and are delineated in the Cybersecurity Law, Data Security Law, and Personal Information Protection Law. (Bailey & Parsheera, 2018, p. 47) The data localization requirements in Vietnam are stipulated in the Cybersecurity Law and the draught decree on data protection, which pertains to Vietnam's proposed privacy legislation. Applying the data localization requirement in Indonesia is exclusively limited to public electronic system operators.

Among the ASEAN Countries, China is the nation that crafted the rigid principles of data localization wherein it states that the data intermediaries should restrict the personal data within the territory of China. The Figure 2 mentioned hereinafter clearly articulates the intensified increase of Data flow across the borders as compared to the data storage. Even though the cross border at the initial point is indicating the spike of data transfer across borders from 2006 and it continued upto 2021.

China's many overlapping data privacy rules have made compliance challenging. The 'Resolution relating to Strengthening the Protection of Information on the Internet' of December 2013 includes general laws for Internet Service Providers (ISPs) and other businesses prohibiting the collection of personal data without consent and the illegal transfer or sale of personal data. The Standardisation Administration and the General Administration of Quality Supervision, Inspection, and Quarantine published new national standards prohibiting overseas data transfers without user consent, government permission, or other explicit legal or regulatory permission the same year. Although voluntary, these standards serve as a "regulatory baseline" for law enforcement and constitute data localization regulations for all businesses. In a 'Notice to Urge Banking Financial Institutions to Protect Personal Financial Information,' the People's Bank of China (PBOC) prohibits off-shore storing, processing, or analysis of Chinese citizens' financial information. The Ministry of Industry and Information Technology (MIIT) prohibits data collection without consent or a 'specific and clear purpose.'

The imposition of data localization rules is mandated by Government Regulation 82 of 2012, which pertains to the operation of electronic systems and transactions in Indonesia, commonly referred to as the Indonesia OEST Regulation. According to Article 17(2) of the OEST Regulation in Indonesia, it is mandated that operators of electronic systems for public services are required to establish data. Centres and disaster recovery centres within the country. This requirement serves the objectives of facilitating law enforcement, safeguarding data, and upholding Indonesia's national sovereignty over the

personal information of its citizens. This provision results in the imposition of both local copy and local action obligations. Ministerial Regulation No 20 of 2016, also known as the Protection of Personal Data in Electronic Systems (PPDES) Regulation in Indonesia, was enacted under Article 15(3) of the Indonesia Online Electronic Systems and Transactions (OEST) Regulation. According to Article 22 of the Indonesia PPDES Regulation, operators of electronic systems in Indonesia must collaborate with relevant authorities by providing specific information regarding transferring personal data outside of Indonesia. However, it remains to be seen whether obtaining approval from these authorities is necessary for such transfers. Article 22 of the relevant legislation prohibits transferring personal data from Indonesia to other jurisdictions, albeit with specific qualifications.

Furthermore, it should be noted that according to Article 17(1) of the Indonesian PPDES Regulation, there is a stipulation that mandates the physical presence of data centres and disaster recovery centres inside the borders of Indonesia. This need applies explicitly to operators of electronic systems utilised for public services, with the primary objective of ensuring the adequate safeguarding of personal data. This provision contributes to the stipulations on local copy and local action outlined in Article 17(2) of the Indonesian OEST Regulation.

To get a clear understanding of the relevant aspect, A comparative analysis of the data localization principles is to be mentioned so that the present situation can be manifested. Table 1 highlights the localization principles prevailing in the ASEAN Countries based on data processing and data transfer from one country to another. Table 1 summarises the localization standards that each of the 10 ASEAN member states must adhere to. Generally, there is now a moderate data localization level among the ASEAN Member States. There has been some convergence regarding the restrictions placed on the international transfer of personal data due to several ASEAN Member States' imposition of data protection adequacy requirements. These requirements stipulate that a data controller transferring data outside the country must ensure that the personal data will receive comparable protection in the country where it is being transferred. However, requirements for local processing continue to be the exception rather than the rule. On the other hand, the local processing criteria adopted up until this point have vague and open-ended wording, which can encompass various data controllers and data types.

8.0 Data Localization: Its Impact on the ASEAN Digital Economy

The Association of Southeast Asian Nations (ASEAN) member nations have made an effort to encourage the digitalisation of the area with the release of the ASEAN Digital Masterplan 2025 (ADM 2025). Data is crucial to this digital transformation process because it underpins and produces every interaction in the digital sphere. Southeast

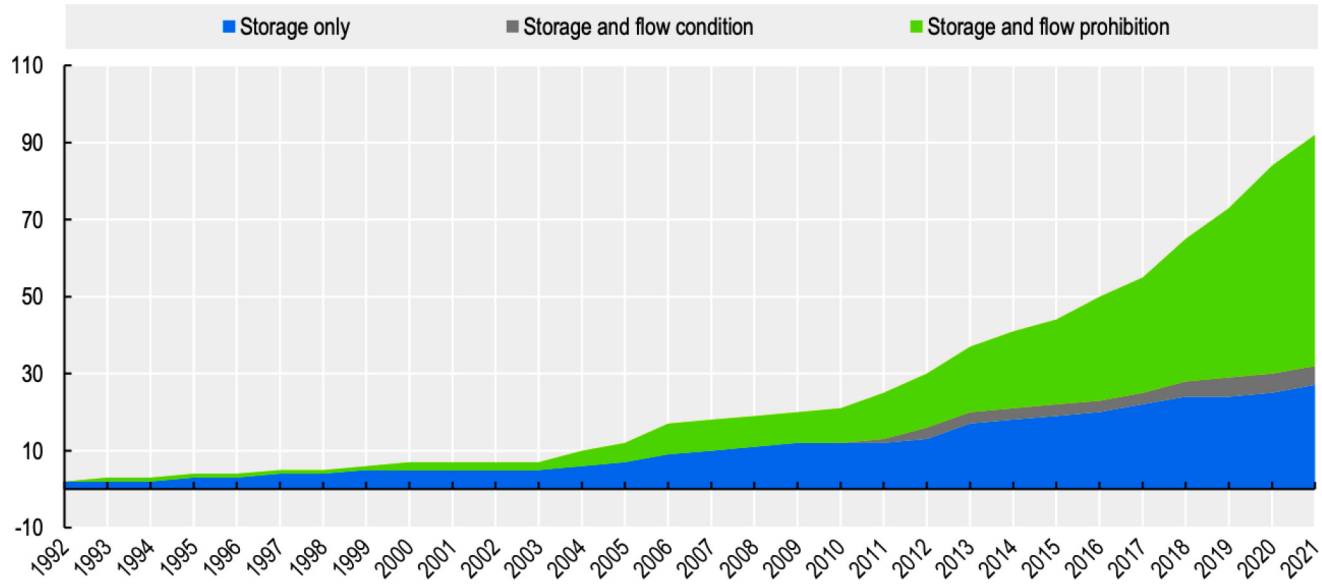


Figure 2. Data Flow Across Borders and its purposes.

Table 1. Comparative Analysis of Data Localization Principles Among the ASEAN Countries

Countries	Local Processing	Transfer Limitation
Brunei		
Indonesia	**Local copy and action (Indonesia OEST Regulation).**	**Qualified restriction (Indonesia PPDES Regulation).**
Cambodia		
Laos		
Malaysia		**Qualified restriction (Malaysia PDPA).**
Myanmar		
Philippines		**Qualified restriction (Philippines DPA).**
Singapore		**Qualified restriction (Singapore PDPA).**
Thailand		**Qualified restriction (Thailand PDPA).**
Vietnam	**Local copy Vietnam Law on Cybersecurity Local copy and action (Vietnam Decree 72).**	

Asian nations have increased their attempts to create their own data governance policies due to realising the importance of data. For instance, robust data protection laws have been passed in Thailand, Singapore, and Indonesia. By 2024, Vietnam also plans to publish a complete version of its data privacy law (Abdurrohim, 2022, p. 24).

Even though data flows drive digitalisation, several ASEAN members have tightened restrictions on cross-border data flows and even implemented data localization rules. For instance, Vietnam requires foreign telecom and technology businesses to retain consumer data locally. Indonesia requires data localization in specific industries, such as the financial industry, and demands that all public sector data be held there. Although Thailand or the Philippines have not addressed data localization explicitly, it may be covered under their data privacy rules if interpreted broadly. According to reports, Cambodia will also shortly announce data localization requirements. (Tholens, 2017, p. 72)

National security and digital sovereignty are the key motivators for growing data localization norms among Southeast Asian nations. Cross-border data flow restrictions might not necessarily slow down the region's digitisation process; instead, they could be a double-edged sword.

While several Southeast Asian nations have similarities with the General Data Protection Regulation (GDPR) of the European Union regarding their data protection initiatives, they have different motivations for doing so than the EU. The EU bans cross-border data transfers because privacy is fundamental to human rights. Southeast Asian nations, in contrast to the EU, evaluate data from the standpoint of sovereignty rather than individual rights. They contend that maintaining control over the data produced in and held by their nations is essential to state sovereignty and national security.

For instance, the minister of communication and information technology for Indonesia, Johnny G. Plate, has said categorically that national sovereignty pertains to data control. He also asserted that safeguarding digital and data sovereignty and avoiding the establishment of a digital colony was essential to promoting and upholding Indonesia's independence during the celebration of Indonesia's Independence Day (Binardy, 2021, p. 54). Likewise, Malaysia's Ministry of Communications and Multimedia's Mohammad Mentek stated that maintaining data sovereignty is a crucial objective for his nation as it develops the current legal and policy frameworks on data. (Putra, 2022, p. 5527) Vietnam has prioritised protecting national sovereignty as a top priority while constructing its data governance. Vietnam has passed legislation to ensure that the data of the Vietnamese people stays within and under its control to increase its internet sovereignty. Southeast Asia is one area with the fastest data centre expansion rate. Southeast Asia has 195 data centres in total as of this month. The data centre market in the area was estimated to be worth $8.71 billion in 2021 and $12.34 billion by 2027, according to a recent market analysis by Arizton. Southeast Asia will soon overtake North America as the world's largest region for co-locating data centres. Restrictions on unhindered data transfer across international borders are partly to blame for this rapid increase. For instance, establishing the data localization law has played a significant role in Vietnam's market growth of data centres. Similarly, the government's mandates for data localization have increased demand for regional data centres in Indonesia.

Expanding data centres in Southeast Asia will hasten the region's digitalisation, which is significant. Data centres are

vital parts of the IT infrastructure and are crucial to the digital transformation. The physical foundation of digital existence is made up of these facilities. People in Southeast Asia will probably have access to faster, more dependable internet speeds, technology innovation will be further promoted, and businesses in the area will find it simpler to connect, move to the cloud, and digitalise their operations and services as a result of the growing support for data centres. While limiting cross-border data flows encourages the development of data centres, which can help with digitalisation, the same data localization standards and restrictions might make it more difficult for the region to achieve its digitalisation goal. Data flows that cross borders are essential to a digital economy. Because restrictions on cross-border data transfers are seen as significant obstacles to digital trade, they may also obstruct ASEAN's transition to a digital economy.

Additionally, restrictions on international data transfers impede ASEAN's growth into a digital society. Since it facilitates the digitalisation of every aspect of daily life, from education and entertainment to healthcare and transportation, the Internet of Things (IoT) is the cornerstone of a digital society. Regulations that impede the implementation of IoT may unavoidably hamper Southeast Asia's digital transformation since they restrict international data flows.

By 2025, ASEAN pledged a digital economy and society in the region. Although Southeast Asian nations have stepped up their efforts to control data—seen as the new oil in today's world—many still prefer to impose restrictions on the unfettered data movement across their borders. Additionally, it is more challenging for Southeast Asian nations to make concessions and loosen the rules because restrictions on international data transfers are the product of worries about national security and state sovereignty. The restrictions will undoubtedly create more obstacles in society as data localization serves as a double-edged sword for the digital economy.

9.0 India's Digital Personal Data Protection Act, 2023: A New Feather in the Cap

After a long hassle, India finally entered the spectrum of data localization under the aegis of the Digital Personal Data Act 2023. Reserve Bank of India, in 2021, issued a notification to localise the citizens' financial data within India's territorial ambit. The new act whispered the notion of data localization under Section 16 of the Act, but not in a positive aspect but in a negative connotation. The New Act of India stipulates that restrictions can be imposed by the Central Government based on the conditions that the government will make after that. Furthermore, The Act allows the legislature to maintain a higher degree of restriction on disseminating personal data across borders.

Fintech applications like Google Pay, Amazon Pay, PhonePe, etc., are making life more accessible for individuals. With the help of a phone, by a single click, one can reduce the hassle of standing in a long queue, ultimately saving people's time and energy. But the pertaining question that evolves within this precinct of Fin Tech generation is outsourcing personal and financial data across borders. It would be imperative for any nation to solely depending on their resources. This is the main agenda of the recent G20 Summit wherein India claimed to be the torchbearer of the FinTech revolution. India's fintech industry valuation is projected to surpass $150–$60 billion by 2025. Another report predicts that the Indian fintech market will reach $2.4 trillion by 2025 making it one of the fastest-growing sectors in India.

The government introduced the central bank's digital currency and a new crypto tax policy in 2022. Banks increasingly invest in and collaborate with fintech start-ups to develop new products and services. Customers can pay bills, recharge their phones, and make purchases using a variety of fintech applications on their mobile devices. The Reserve Bank of India has issued a new and remarkable framework known as "UPI123Pay" to enable offline digital payments without an internet connection. India has a golden opportunity to prove it is a global fintech powerhouse. With an adoption rate of 87% compared to the worldwide average of 64%, India has surpassed the established nations in this area. The National Payments Corporation of India has already begun internationalising the Unified Payments Interface (Jha, 2023, p. 5) Although the Fintech company accelerates the Indian economy, it is against the contours of Data localization and data protection of the people of India.

10.0 Conclusion and Suggestion

There are two essential facets regarding Data localization: one is economic integration, and another is securing the informational privacy of individuals. Both these facets stand as a predicament for the stable structure and economy of the country, and it is required to be harmonised as well. It is evident from the preceding discussion as to what extent

the digital economy catalyses the growth of the economy of ASEAN Countries. Data localization is the practice that acts as a double-edged sword that curtails data breaches and also diminishes the spark of the digital economy. The impact is particularly pronounced in future growth and opportunity areas, such as digital trade, e-commerce, global value chains, digital services, and fintech innovation. Data localization focuses on one facet of the shifting landscape, while numerous related threads run on parallel tracks, separated by industry and sectoral silos and governed by rules established for a world based on physical products and analogue services. These frameworks are demonstrated to need to be improved for the digital economy. The country members of the ASEAN Community, like Malaysia, Vietnam, China, and Indonesia, inculcated the principles of data localization in their data governance framework. As a new actor in data governance, India applied the data localization principles to restrict financial data but not through a comprehensive mechanism. The New Digital Personal Data Protection Act 2023 cast the task to the government of India to articulate the implementation of data localization principles. Implementing data localization principles within the ambit of data governance is a vital step towards securing the Right to privacy of individuals but at the stake of the country's digital economy. If data localization rules are put in place and the free flow of data is limited, the digital environment may never be able to reach its full potential.

Where data localization regulations apply, a data localization strategy is required. The increasing heterogeneity of data localization laws in Asia is causing difficulties for businesses (so much so that 'data residency as a service company has emerged, offering solutions to help regulated industries remain compliant). Data migration is typically a costly and time-consuming endeavour that necessitates meticulous planning. The question is whether and when data migration should be implemented for Asian jurisdictions with data localization laws, given that most international businesses store their data centrally across the Asian region. The absence of a data localization strategy could have economic repercussions. Existing enterprise-wide data storage and hosting arrangements may only be able to be leveraged if existing service providers can provide in-country storage arrangements. It may also make it problematic to synthesise regional data storage arrangements. At this conjecture, the following suggestions can be placed for consideration to make a harmonious construction of these two diverse facets:

1. A well-balanced data localization regulation could safeguard the privacy of Indian consumers and the country's national and economic interests.
2. Local organisations may gain a competitive advantage by storing data locally. However, it is equally essential for the government and regulators to enact adequate measures to ensure that establishing data privacy barriers does not discourage global corporations from investing in the country.
3. Bilateral Agreements can serve as an essential approach to regulating data localization liberally.
4. The government should act as an intermediary to facilitate the digital liberty of the individual and maintain individuals' privacy.
5. The relevance of the accountability principle and the proportionality test described in the OECD Privacy Guidelines for evaluating data localization initiatives should be taken.
6. Exploring more effective strategies to tackle cross-border data challenges,

such as establishing trade agreements and multilateral frameworks that facilitate the secure and authorised movement of data. Data localization principles of the European Union should be evaluated for further research. It is imperative to have a consonance of the principles of the European Union and the trends of the ASEAN community subjected to the nation's economic sustainability.

References

Abdurrohim, M. (2022). ASEAN digital masterplan: Responding cyber security dilemma in the post-covid era. *Global Focus*, *2*(1), 17–26. https://doi.org/10.21776/ub.jgf.2022.002.01.2

Abidin, C. (2020). Mapping internet celebrity on tiktok: Exploring attention economies and visibility labours. *Cultural Science Journal*, *12*(1), 77–103. https://doi.org/10.5334/csci.140

Ayaburi, E. W. (2022). Understanding online information disclosure: Examination of data breach victimization experience effect. *Information Technology & People*. https://doi.org/10.1108/itp-04-2021-0262

Bailey, R., & Parsheera, S. (2018). Data localisation in india: Questioning the means and ends. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3356617

Binardy, Y. A. (2021). Legal protection arrangements in indonesia for privacy rights in cases of personal data leakage. *International Journal of Social Science and Human Research*, *04*(12). https://doi.org/10.47191/ijsshr/v4-i12-56

Belova, L. (2021). Sharing economy: The business model of the digital economy in the COVID-19 period. *World Economy and International Relations*, *65*(5), 87–94.https://doi.org/10.20542/0131-2227-2021-65-5-87-94

Carbonell-Nicolau, O. (2024). Inequality and bipolarization-reducing mixed taxation. *Mathematical Social Sciences*. https://doi.org/10.1016/j.mathsocsci.2024.11.001

Chen, S. Tran, K. T., Xia, Z., Waseem, D., Zhang, J. A., & Potdar, B. (2023). The double-edged effects of data privacy practices on customer responses. *International Journal of Information Management*, *69*, 102600. https://doi.org/10.1016/j.ijinfomgt.2022.102600

Collignon, S. (2012). Rebalancing the global economy. *Global Policy*, *3*(2), 154–168. https://doi.org/10.1111/j.1758-5899.2011.00115.x

Dugar, S., & Mitra, A. (2016). Bertrand competition with asymmetric marginal costs. *Economic Inquiry*, *54*(3), 1631–1647. https://doi.org/10.1111/ecin.12328

Fatima, Talat. (2017). *Cyber Law in India*. Kluwer Law International.

Fraser, E. (2016). Data localisation and the balkanisation of the internet. *SCRIPTed*, *13*(3), 359–373. https://doi.org/10.2966/scrip.130316.359

French, C., Carr, B., & Lowery, C. (2020). Data Localization: Costs, Tradeoffs, and Impacts Across the Economy. *Institute of International Finance*, 1–10. https://www.iif.com/portals/0/Files/content/Innovation/12_22_2020_data_localization.pdf

Gon Kim, J., Lee, J., & Kim, J. (2020). Digital economy: A new prospect for korea's new southern policy. *Korea Institute of International Economic Policy*, 1–5. https://www.kiep.go.kr/gallery.es?mid=a10105040000&bid=0007&list_no=5114&act=view&act=view&list_no=5114&cg_code=

Greenleaf, G. (2017). Asian Data Privacy Laws: Trade and Human Rights Perspectives. Oxford University Press.

Hartung, T. (2018). Making big sense from big data. *Frontiers in Big Data*, *1*. https://doi.org/10.3389/fdata.2018.00005

Ichihashi, S. (2021). Competing data intermediaries. *The RAND Journal of Economics*, *52*(3), 515–537. https://doi.org/10.1111/1756-2171.12382

Jha, K. K. (2023). Digital payments and e-rupi for the new age india: An overview. *Interantional Journal of Scientific Research in Engineering and Management*, *07*(09). https://doi.org/10.55041/ijsrem24811

Kienscherf, M. (2022). Surveillance capital and post-fordist accumulation: Towards a critical political economy of surveillance-for-profit. *Surveillance & Society*, *20*(1), 18–29. https://doi.org/10.24908/ss.v20i1.14235

Kuner, C. (2023). Protecting EU data outside EU borders under the GDPR. *Common Market Law Review*, *60*(Issue 1), 77–106. https://doi.org/10.54648/cola2023004

Kingsbury, D. (2003). The political economy of cross-border relations. *South East Asia Research*, *11*(3), 269–296. https://doi.org/10.5367/000000003772657373

Klobuchar, A. (2021). Antitrust: Taking on monopoly power from the gilded age to the digital age. Knopf Doubleday Publishing Group.

Law, K. (2024). Fintech and minority welfare: Evidence from the mortgage market. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4795450

Law, K., & Mislang, N. (2022). The heterogeneity of bank responses to the fintech challenge. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4069077

Marek, P. (2008). Financial crisis, fall and financial theory. *European Financial and Accounting Journal*, *3*(4), 4–5. https://doi.org/10.18267/j.efaj.86

Permana, R. B. (2019). Disciplining data localisation measure: Approach through ASEAN agreement on e-commerce. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3497567

Putra, Y. P. (2022). Comparison of personal data protection laws using narrative policy framework between indonesia, malaysia, and japan. *NEGREI: Academic Journal of Law and Governance*, *2*(2), 99. https://doi.org/10.29240/negrei.v2i2.5527

Shi, Y. (2022). Digital economy: Development and future. *Bulletin of Chinese Academy of Sciences*, *37*(1), 78–87. https://bulletinofcas.researchcommons.org/journal/vol37/iss1/11. Available from: https://doi.org/10.16418/j.issn.1000-3045.20211217002

Soni, D. Y. P. (2019). Global Village and the Economy. United Kingdom: Xlibris UK.

Southeast Asia Data Center Construction Market- Industry Outlook and Forecast 2023-2028. (2023). Arizton Advisory and Intelligence.

Tholens, S. (2017). Winning the post-war: Norm localisation and small arms control in Kosovo and Cambodia. *Journal of International Relations and Development*, *22*(1), 50–76. https://doi.org/10.1057/s41268-017-0098-9

The political writings of harold D. lasswell: Psychopathology and politics; politics—who gets what, when, how; democratic character. by harold D. lasswell. (glencoe, illinois: Free press. 1951. pp. 525. $5.00.). (1951). *American Political Science Review*, *45*(3), 936. https://doi.org/10.1017/s0003055400302453