ACI Research Paper #17-2023

Data Regulations in Vietnam

Thi Hong Hanh PHAN

Thi Hang BANH

August 2023

Please cite this article as:

Phan, Thi Hong Hanh and Thi Hang Banh, "Data Regulations in Vietnam", Research Paper #17-2023, *Asia Competitiveness Institute Research Paper Series (August 2023)*

DATA REGULATIONS IN VIETNAM

Phan Thi Hong Hanh and Banh Thi Hang[1]

August, 2023

Abstract

As data plays a critical role in the global economy, governments are increasingly focusing on data regulations to address human rights, national security, and privacy concerns. Vietnam's digital economy has experienced significant growth, prompting the government to implement laws and regulations to protect data, driven by national security considerations and international trade obligations. This research paper analyzes Vietnam's data protection regulations, particularly on data localization, cross-border data flow, and privacy and data protection. A comparative analysis is conducted between Vietnam and major economies such as the United States, the European Union, and China. The paper concludes that Vietnam follows a limited model, with data security intertwined with cybersecurity and national interests. However, due to external pressures and international obligations, Vietnam faces challenges in imposing stringent data regulations independently. The findings highlight the significance of national security as a justification for data governance across different countries.

[1] Asia Competitiveness Institute, Lee Kuan Yew School of Public Policy, National University of Singapore. PH: hanh.phan@u.nus.edu, HB: hangbanh@nus.edu.sg

1. Introduction

Data has become increasingly crucial in today's interconnected world, shaping the landscape of the contemporary global economy. In an era marked by remarkable advancements in communication and computing technologies, the volume of data generated, transmitted, and stored on a daily basis has reached unprecedented levels. This exponential growth in digital trade has positioned it as the fastest-growing sector of global trade, surpassing trade in goods, and contributing considerably to global economic expansion, with an annual growth rate of 5.4% (Nakanishi & Hori, 2023). To effectively operate within the international digital market, businesses that rely predominantly on data for their business models require continuous and dependable access to data, as well as seamless data transfer among corporate entities and across the global business ecosystem.

As the global economy becomes increasingly involved in data collection, storage, and transfer, non-economic aspects such as the protection of human rights (including privacy and personal security) and national security have emerged as significant concerns. Consequently, governments worldwide are placing increased emphasis on data governance. Different nations adopt varying approaches to data regulations, prioritizing different core values and interests. For example, the United States follows a liberal model of data governance, driven by its dominant position in the data market. Conversely, China enforces stringent data regulations to safeguard national security. The European Union, recognizing the importance of safeguarding privacy and protecting personal data as fundamental rights, has enacted a comprehensive framework called the General Data Protection Regulation (GDPR).

The robust growth of Vietnam's digital economy can be attributed to the substantial development of its digital infrastructure and cyber economy. According to the Ministry of Information and Communications (MIC, 2023), the digital economy accounted for 14% of Vietnam's GDP as of 2022. This contribution is expected to rise significantly, aiming to reach 30% of GDP by 2030 as outlined in the “National Digital Transformation Program to 2025, with a vision towards 2030”. Consequently, there has been a noticeable increase in online economic and social activities within Vietnam, with 94.2 million smartphone users and 82.2 million mobile broadband subscribers recorded in 2022, encompassing approximately 74% of the national population (MIC, 2022).

As the digital economy expands, the Vietnamese government has recognized new concerns and challenges, leading to the implementation of laws and regulations for data protection in recent years, such as the Cybersecurity Law and Personal Data Protection Decree. The approach taken by Vietnam towards data governance is driven by national security considerations, with the government perceiving cyberspace as the "fifth space, the fifth battlefield, the fifth realm of a nation, alongside land, air, sea, and space” (To, 2021). Furthermore, the enactment of data regulations is seen as an essential obligation for the Vietnamese government due to the country's deepening integration into international trade through preferential trade agreements. These trade agreements invariably include provisions related to data regulations, necessitating Vietnam's adherence to them.

The primary objective of this paper is to provide an up-to-date overview of the data regulations in Vietnam, considering the recent introduction of personal data protection regulations. Furthermore, it aims to assess the implications of these regulations on businesses, government entities, and other stakeholders by analyzing and contrasting Vietnam's regulatory approach with that of other countries and other free trade agreements that Vietnam is a member of.

This research paper analyzes the existing regulatory framework for data protection in Vietnam, focusing on three key aspects: data localization, cross-border data flow, and privacy and data protection. After giving an overview of key data regulations in Section 2, Section 3 will evaluate the alignment between Vietnam's domestic data regulations and its international obligations as stipulated in preferential trade agreements such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and Regional Comprehensive Economic Partnership (RCEP). Section 4 will compare Vietnam's data regulation model with that of other major economies, including the United States, the European Union, and China.

2. Fundamental data regulations in Vietnam

Data governance has gained significant importance among policymakers due to the rapid growth of the digital economy, raising concerns regarding national security and data privacy. Countries have adopted diverse approaches to governing data, which can be classified into three distinct models. This section briefly describes the three data governing models and then examines Vietnam's data model and its fundamental data regulations.

2.1. Taxonomy of data regulations

Data localization

The unrestricted flow of cross-border data has become a subject of concern due to the increasing number of countries adopting data localization requirements worldwide. Governments are imposing these mandates for various reasons, each serving distinct public policy objectives. These conditions are often put in place to protect data, ensure national security, expand regulatory control, and strengthen data security measures. Additionally, these measures are intended to safeguard and boost domestic digital industries (Fefer et al., 2021).

Data localization requirements can manifest in both implicit and explicit forms. Implicit measures involve limitations on cross-border data flow, necessitating local data storage and processing. On the other hand, explicit data localization regulations explicitly mandate that data be stored and/or processed on servers within the jurisdiction (González, 2022). In the context of trade agreements, data localization provisions aim to prevent the use of computing facilities' locations as a prerequisite for conducting business in a particular territory.[2] In general, data localization requirements can be broadly classified into four distinct categories:

(i) No requirement for data localization but guarantee access to data.

[2] Provisions in CPTPP, RCEP and some ASEAN initiatives

(ii) Data localization requirement but no restriction on the cross-border data transfer.

(iii) Data localization requirement with conditional transfer and access conditions.

(iv) Data localization and processing requirement with a prohibition on cross-border data transfer or ad-hoc authorization (González, 2022).

Cross-border data flow, and privacy and data protection

The regulations of cross-border data flow and data protection can be classified into three distinct models: the open model, the conditional model, and the limited model (Ferracane & Marel, 2021) (Table 1). These models vary in terms of the cross-border transfer of data and the protection of users' data. The open model represents a broad approach that lacks a comprehensive framework for regulating cross-border data transfers and ensuring data protection. Under this model, there are no significant restrictions on cross-border data transfers, often facilitated through preferential trade agreements. Companies are given flexibility to self-regulate and take responsibility for cross-border data transfers. However, within this model, data subjects are granted limited rights regarding data processing, as countries adhering to this model have yet to establish comprehensive data protection regulations.

Table 1. Three models of data regulations

	Cross-border data transfers	Data protection
Open model	Self-certification; self-assessment schemes; ex-post accountability; trade agreements and plurilateral/bilateral arrangements as only means to regulate data transfers.	Lack of comprehensive data protection framework; lack of informed consent; privacy as a consumer right.
Conditional model	Conditions to be fulfilled ex-ante, including adequacy of the recipient country, binding corporate rules (BCR), standard contract clauses (SCCs,) data subject consent, codes of conduct, among others	Wide data subject rights; data subject consent; right to access, modify and delete personal data; establishment of data protection authorities (DPAs) or agencies; privacy as fundamental human right.
Limited model	Strict conditions including bans to transfer data cross border; local processing requirements: ad hoc government authorization for data transfers; infrastructure requirements; ex-ante security assessments.	Extensive exceptions for government access to personal data; privacy vs security and social order.

Source: Ferracane and Marel (2021).

The conditional model, as the second approach, enables cross-border data transfer by imposing specific conditions. Such transfer is permitted on the condition that certain requirements are fulfilled, including ensuring adequate data protection in the recipient country, obtaining consent from data subjects, implementing standard contract clauses, adhering to binding corporate rules, and complying with codes of conduct. Countries that adopt this model acknowledge data protection as a fundamental right and have therefore established comprehensive regulatory frameworks for data protection.

The limited model is frequently embraced by nations wherein data privacy and protection concepts are intricately tied to cybersecurity and considered national security matters (Gao, 2019). To bolster cybersecurity measures and uphold national security interests, cross-border data transfers within the framework of this model are subject to stringent restrictions, encompassing measures such as prohibitions, case-by-case governmental authorizations, and pre-emptive security assessments. Regarding data protection, this model allows for extensive exemptions permitting government intervention in domestic data processing. It is worth noting that a country falls into the classification of this model if it grants considerable exceptions for authoritative access to data, even if it maintains a comprehensive framework for data protection (Ferracane & Marel, 2021).

Vietnam follows a limited model in its approach to data regulation, which encompasses data localization requirements, conditional transfer, and access conditions. These aspects will be thoroughly examined in the following sections.

2.2. Overview of data governance in Vietnam

Since 2006, Vietnam has prioritized personal data security, evident through the introduction of the Law on Information and Technology. This law mandates individuals and companies to inform and obtain consent from data subjects before collecting and processing their personal data, thus guaranteeing data protection. Subsequent legal documents like the Law on Cyberinformation Security and Decree 14 on E-Commerce have consistently reinforced this regulation.

As online economic and social activities have increased in volume, the importance of data protection and privacy has correspondingly grown. To assert control over data and safeguard both data protection and national interests, Vietnam has adopted a limited data model, incorporating external and internal safeguards into its data regulations (Table 2). The Cybersecurity Law (CSL), effective since 2019, along with related Decrees like Decree 53 and Decree 13, are of utmost importance, addressing crucial aspects such as data localization, cross-border data flow, and privacy protection (Burri, 2021).

Data localization

Under the CSL, both domestic and foreign companies collecting, analyzing, and processing personal data of Vietnamese users must store that data within Vietnam's territory within a specified timeframe. Additionally, the Law mandates that companies establish offices or representatives in Vietnam, strengthening the government's authority over Vietnamese user data and ensuring accountability in case of violations.

However, from a business perspective, the localization requirements come with significant costs and risks. For example, companies must allocate additional funds to build infrastructure for data storage. Moreover, since a single jurisdiction has complete control over the data, it could potentially lead to censorship by restricting access to platforms and disrupting the flow of cross-border data if companies fail to comply with local regulations (UNCTAD, 2016).

Table 2. Key Laws on data regulation in Vietnam

KEY LAWS ON DATA REGULATION	REGULATIONS UNDER THE LAW
Law on Information and Technology	
• Effective on 1 January 2007. Amended in 2017 • Key data regulation content: Data subjects must be informed of and give consent to their personal data to be collected and processed.	• **Decree 14 on E-Commerce (2021):** Individuals and firms doing business on e-commerce platforms must take responsibilities to protect users' personal data including obtaining their consent to collect personal data.
Law on Cyberinformation Security	
• Effective on 1 July 2016 • Key data regulation content: Transparent information, communication and modalities for the exercise of the rights of the data subject.	
Law on Cybersecurity	
• Effective on 1 July 2019 • Key data regulation content: Data localization and establishment of local company presence	• **Decree 53 guiding Cybersecurity Law (2022):** Specific guidance on data localization and establishment of local office requirements. • **Decree 13 on Personal Data Protection (2023):** Regulations on data protection and cross-border data transfer.

Source: Government's documents.

Foreign companies and governments have openly voiced their concerns over the localization regime in the Cybersecurity Law (USTR, 2021). Furthermore, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the Regional Comprehensive Economic Partnership (RCEP) Agreement, both of which Vietnam is a member of, explicitly prohibit data localization. In response to this pressure and to align with practical considerations, the Vietnamese government has adjusted the data localization requirements.

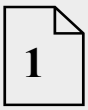
According to Decree 53 guiding the Cybersecurity Law, domestic firms are mandated to localize data in Vietnam for at least 24 months. However, foreign companies operating in ten specific sectors are only required to store data and establish a local presence in Vietnam if they violate cybersecurity laws and regulations and fail to cooperate in preventing incidents after receiving notices from the Ministry of Public Security (MPS) (Boxes 1 and 2). In such cases, the MPS will issue a data localization requirement to the foreign company, allowing them 12 months to comply by localizing their data in Vietnam. If a firm fails to comply with the MPS's order, they must inform the Ministry and will be granted a 30-day period to rectify the non-compliance. It should be noted that the definition of prohibited activities in the CSL is somewhat ambiguous, encompassing acts such as anti-state propaganda, inciting violence, and undermining public order. The definition of offences is broad and subject to the discretion of authoritative agencies.

Box 1. Sectors in which foreign companies operating in Vietnam are subject to data localization (Decree 53)

1) Telecommunications
2) Data storage and sharing on cyberspace
3) Providers of local or international domain names for users in Vietnam
4) E-commerce
5) Digital payment
6) Payment intermediaries
7) Online transportation services
8) Social media platforms
9) Online games
10) Other information provision, management, or operation services on cyberspace through messaging, voice calls, video calls, email or online chat

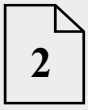
**Notes: Only foreign companies which operate in these 10 sectors and violate cybersecurity regulations are required to store data in Vietnam.*

Box 2. Types of data to be stored in Vietnam (Decree 53)



Personal data of Vietnamese users

- Data in the form of symbol, letter, number, picture, sound, or similar forms to identify a person



Data created by Vietnamese users

- Account name
- Duration of account usage
- Credit card information
- E-mail account
- IP account
- Most recent log-in
- Registered phone number for account

Data on relationships of Vietnamese users

- Friends
- Groups of which they are a member

Cross-border data flow

To protect Vietnamese users' personal data, measures have been taken to control data transfers. In 2021, the government drafted the Decree on Personal Data Protection, aiming to regulate transborder data transfers. The initial draft adopted a stringent ex-ante accountability approach, potentially impeding the free flow of information. This approach required four simultaneous conditions for transferring personal data of Vietnamese users: (i) obtaining consent from data subjects, (ii) storing the original data in Vietnam, (iii) providing evidence of equivalent data

protection at the destination, and (iv) obtaining written agreement from the Data Protection Commission.

However, a significant shift in the approach to data transfers occurred between the first draft and the final version of Decree 13, signed on April 17, 2023. The ex-ante accountability approach was replaced with an ex-post accountability approach, resulting in less restrictive data flows. Data controllers and processors are no longer required to obtain a written agreement from the authority agency before conducting data transfers. Instead, data can be legally transferred out of Vietnam as long as the data processor and controller submit impact assessment reports to the MPS within 60 days of data processing commencement. Following the completion of the data transfer, a written notice must be sent to the Ministry. If the MPS requires additional information, the data processor and controller have 10 days to improve the evaluation reports accordingly (Box 3). The MPS conducts annual inspections of data transfers.

Box 3. Procedures for cross-border data transfer (Decree 13)

STEP 1: Data processor and controller conduct impact assessment reports for cross-border data transfers.
STEP 2: Data processor and controller send the reports to the Department of Cybersecurity and High-Tech Crime Prevention and Control, Ministry of Public Security within 60 days since the data are processed and notify the Ministry upon the successful transfers of data.
STEP 3: The Ministry of Public Security assesses the reports and notifies the data controller and processor of the need to improve the reports.
STEP 4: Data processor and controller have 10 days to amend the reports as required.

Content of evaluation report

- Contact details of data sender and receiver
- Purpose of data transfer
- Data description
- Data protection measures
- Assessment of possible risks relating to data transfer
- Data subjects' consent
- Binding agreement between data sender and receiver

The shift from an ex-ante to an ex-post accountability approach in data transfer policy was largely driven by pressure from foreign governments with business interests in Vietnam and the local business community (USTR, 2021). Although the ex-ante approach can effectively prevent data breaches by requiring prior approval from the Ministry of Public Security (MPS), it can also be time-consuming and inflexible (Barnes, 2023). This requirement may not always be adaptable to urgent situations. However, replacing the ex-ante approach with ex-post accountability does not diminish the policy's effectiveness, as this approach serves as a deterrent by imposing severe penalties (such as data transfer termination) for non-compliant behaviour. Nonetheless, one significant drawback of the ex-post approach is its limited effectiveness in preventing data breaches since it only addresses non-compliance after it has occurred.

The MPS will require data processor and controller to terminate data transfer if they: (i) use the data to jeopardize Vietnam's national interest and security; (ii) fail to comply with the MPS's order to improve the impact assessment reports, or (iii) cause the loss of personal data of

Vietnamese users. Although the Decree has facilitated cross-border data transfer by removing restrictive provisions, data controllers and processors must exercise caution due to the broad and ambiguous definition of national interest. Skilful navigation is essential to avoid the risk of termination.

Privacy and data protection

Decree 13 on Personal Data Protection establishes a framework for safeguarding the personal data of Vietnamese users. It outlines the rights of data subjects and the duties of data processors and controllers. This Decree grants individuals a wide range of rights, including being informed about data processing, giving consent, withdrawing consent, accessing, modifying, and deleting personal data, and the right to lodge a complaint for misuse or loss of personal data. These extensive rights provided to data subjects in Decree 13 closely resemble those outlined in the European Union's General Data Protection Regulation (GDPR).

However, there are certain circumstances where data processing can be carried out without obtaining consent from data subjects. For instance, data processors and controllers can process personal data without consent in emergencies to protect the data subject's life, safeguard national interests, maintain social order, or at the request of competent agencies.

To ensure compliance with privacy and data protection regulations, foreign and domestic companies are required to appoint a personal data protection officer or establish a personal data protection agency. The officer/agency is responsible for ensuring the rights of data subjects and reporting to the government's data protection agency. Micro, small, and medium enterprises (MSMEs) and start-ups are exempted from having a personal data protection agency/officer for the first two years after their establishment. MSMEs and start-ups that directly engage in personal data processing are exempt from this regulation.

3. Comparing Data Regulations in Vietnam's Domestic Regulations and Multilateral Agreements

By 2021, about 55% of preferential trade agreements contain data-related provisions (Burri, 2021). These data regulations within free trade agreements aim to foster the harmonization of fragmented data regulatory frameworks across different countries worldwide. Among the prominent free trade agreements in the Asia-Pacific region, the CPTPP and RCEP stand out, each encompassing data regulations with varying levels of commitment and language.

Vietnam is a member of the CPTPP, the RCEP, and the Association of Southeast Asian Nations (ASEAN), which has implemented data regulations for intra-bloc operations. Prior to joining these agreements, Vietnam had developed domestic data regulations. As a result, this section aims to assess Vietnam's alignment of domestic data regulations with those in the CPTPP, RCEP, and ASEAN initiatives, in order to examine how the country harmonizes its domestic policies with its multilateral commitments.

Comparison in key areas of data regulations

This section compares the data regulations in Vietnam's domestic laws to those in other multilateral agreements that Vietnam is a party to, focusing on three critical areas: data localization, data flow, and data protection. In the context of data-related initiatives in the Association of Southeast Asian Nations (ASEAN), the analysis centers around several key regional frameworks, including the ASEAN Framework on Personal Data Protection (2016), ASEAN Framework on Digital Data Governance (2018), and ASEAN Data Management Framework (2021) (Jonathan Lim, 2021), as well as the ASEAN Agreement on E-Commerce (2019) (Table 3).

Table 3. Data regulations in Vietnam, CPTPP, RCEP and ASEAN initiatives

Domestic laws/ FTAs/initiatives	Data localization	Data flow	Personal Data protection
Vietnam's domestic laws	Law on Cybersecurity: **Data localization is required**. Decree 53 guiding Cybersecurity Law: • Data localization is mandatory for domestic firms. • Foreign firms are required to **store data with conditions**.	Decree 13 on Personal Data Protection: • Allow transfer of data with **ex-post accountability** • **Self-evaluation of transfer of data** by processor and controller is compulsory	Decree 13 on Personal Data Protection: • **Broad rights of data subject**; right to consent to data processing, withdraw consent, access, modify and delete personal data, and claim compensation in case of misuse or loss of personal data. • Firms are required to set up a personal data protection agency. Decree 14 on E-commerce: **Individuals and firms** doing business on e-commerce platforms must **take responsibilities to protect users' personal data** including obtaining their consent to collect personal data.

Domestic laws/ FTAs/initiatives	Data localization	Data flow	Personal Data protection
CPTPP	Article 14.13: • **Prohibits** a CPTPP member from **requiring a business to "use or locate computing facilities** in that Party's territory" as a condition to do business in that country. • Localization regime is permitted only if they do not "constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade" and do not "impose restrictions on transfers of information greater than are required to achieve the objective".	Article 14.11: • **Requires** CPTPP members to "**allow the cross-border transfer of information** by electronic means, including personal information, when this activity is for the conduct of the business of a covered person". • Certain restrictions on data flow are applied in financial services sector for the protection of individual records privacy or confidentiality	Article 14.8: • **Requires** every CPTPP member to "**adopt or maintain a legal framework that provides for the protection of the personal information** of the users of electronic commerce". • Encourage Party to adopt **non-discriminatory practices** for personal information protection and develop mechanisms to **promote compatibility** between different regimes.
RCEP	Article 12.14: • **Prohibits** a Party member from **requiring a covered person to use or locate computing facilities** as a condition to do business in its territory. • An RCEP member can **impose any essential measures** to **protect its security interests** without being disputed by other countries.	Article 12.15: • **Requires** every Party member **not to prevent cross border flow data information** by electronic means for the business activity. • It allows exceptions similar data localization provision on the ground of security interests and without being disputed by other members.	Article 12.8 **requires** RCEP members to adopt or maintain a legal framework to **protect personal information of online users.**
ASEAN initiatives	ASEAN Agreement on E-Commerce (2019) places a **restriction on members not to require** individuals and firms from other member State to **locate computing facilities** in their jurisdiction as a condition to do business except financial services sector.	ASEAN Framework on Personal Data Protection: • Member States will endeavor to **ensure and facilitate the flow of information** among ASEAN members. • The framework is **not applied to matters of national security, sovereignty, public safety, public policy and government activities** that Government perceives suitable to be exempted. ASEAN Framework on Digital Data Governance: • **Facilitates data flows** via the development of clear requirement for data transfers. • Maturity differences and local laws in ASEAN members are taken into account.	ASEAN Framework on Personal Data Protection: Member States will endeavor to **implement domestic regulations to protect the rights of data subject** to consent, notification of data processing, access, correction, and retention of personal data. ASEAN Data Management Framework introduces a working mechanism among countries to **help businesses** to **meet data protection standards**.

Source: Government's websites.

Conformity analysis

In general, multilateral agreements to which Vietnam is a party contain an extensive data governance regime, which includes restrictions on data localization, prohibitions on the ban of data flows, and personal information protection. While both the CPTPP and RCEP set out rules on data localization and data flows, the regulations in RCEP are less strict and broader, and include exceptions based on national security. Personal data protection provisions in RCEP are also less comprehensive than those in CPTPP (ADB, 2022). Data regulations in various ASEAN initiatives are comprehensive but leave considerable room for exemptions, considering member states' political and developmental differences.

As the CPTPP, RCEP, and regional initiatives like the ASEAN Agreement on E-Commerce are legally binding, Vietnam must establish domestic data regulations to fulfill its obligations under these agreements. Initially, conflicts between domestic regulations and international commitments led to overly restrictive provisions on data flows, such as ex-ante accountability for cross-border data transfers in the draft Decree on Personal Data Protection. However, Vietnam has taken progressive steps to align its data-related regulations with international commitments.

The initial data localization provisions in the CSL contradicted the CPTPP, RCEP, and ASEAN Agreement on E-Commerce, which prohibit data localization for businesses from member states. However, the guiding Decree 53 resolved this conflict by aligning domestic legislation with international obligations. It introduced specific conditions for data localization that apply to foreign firms. As a result, only foreign companies that violate CSL are required to store their data within Vietnam.

During the initial stages of drafting data flow regulations, conflicting provisions emerged. While FTAs and ASEAN initiatives mandated party members to facilitate cross-border data flows, early provisions in the Decree on Personal Data Protection created obstacles by requiring written agreements from the Data Protection Commission under the MPS for personal data transfers. However, the final version of the Decree eased this requirement, allowing companies to transfer data after conducting and submitting an impact assessment report to the Ministry.

As the protection of personal information has become a significant concern, Vietnam introduced a comprehensive regulatory framework for this area in Decree 13. Vietnam's domestic regulations on personal data protection closely resemble those outlined in the ASEAN Framework on Personal Data Protection and fulfil the binding obligations of the CPTPP and RCEP, providing a legal framework for safeguarding the personal information of online users.

4. A comparison with other countries

Personal data regulation varies significantly across countries and is influenced by major economies such as the United States (US), European Union (EU), and China. These countries' approaches to domestic regulations also have implications for the relevant provisions in the preferential trade agreements they are members of. Given that Vietnam is bound by trade

agreements initially led by the US as the Trans-Pacific Partnership (TPP), which was then renamed to CPTPP in 2018 after the withdrawal of the US, and by the EU and China through the EU-Vietnam Free Trade Agreement (EVFTA) and the RCEP, it is important to examine how Vietnam aligns its domestic data regulations with international obligations by comparing them to the regulations of these countries.[3] This section aims to analyse and compare data regulations in Vietnam with those of the US, EU, and China, specifically focusing on aspects including data localization, cross-border data flow, as well as privacy and data protection (Table 4).

Data regulations in Vietnam generally follow the limited model, a similar approach to China, where data security is closely tied to cybersecurity, national interest, and security. The Minister of Vietnam's MPS has acknowledged the significance of cyberspace, considering it as important as traditional domains like land, air, sea, and space, and referring to it as "the fifth space, the fifth battlefield, the fifth realm of a nation" (To, 2021). Therefore, safeguarding cyberspace amounts to safeguarding national territory and security.

Like China, Vietnam has established a robust data regulatory framework encompassing data localization requirements, restrictions on cross-border data transfer with specific conditions, and provisions granting government access to personal data. However, Vietnam's data regulations are relatively less restrictive, primarily influenced by its heavy reliance on international trade. This necessitates Vietnam's consideration of pressures from foreign governments and the business community, which hold vested interests in the country (USTR, 2021). Notably, Vietnam has transitioned from an ex-ante to an ex-post approach for cross-border data transfer and has adopted data localization requirements based on the country of origin (domestic vs. foreign), rather than implementing sector-specific regulations like China and the US. These accommodating data-related regulations in Vietnam are perceived as supportive for foreign companies.

[3] The TPP text on data regulations has influenced and been replicated in the CPTPP (Burri, 2021).

Table 4. Main features of data regulations in Vietnam, China, the European Union and the United States

	Vietnam	China	European Union	United States
Data model	Limited model	Limited model	Conditional model	Open model
Data localization	Mandatory for domestic firms Foreign companies in 10 sectors are required to store data only when they violate cybersecurity regulations	"Critical information infrastructure operators" to store "important data" in China; Companies that meet the eligibility criteria for a security assessment must store a copy of all data locally	No provisions for data localization	Strict localization policies for defence-related data
Cross-border data flow	Only one mechanism for data transfer Impact assessment reports of cross-border data transfers must be prepared and submitted to the Ministry of Public Security (MPS) within 60 days of processing data Written notice must be sent to the MPS Upon successful data transfer	Cross-border data transfer is allowed under 3 conditions: (i) Pass a security assessment from China's Cyberspace Authority (CCA) (ii) Standard contractual clauses between exporter and recipient (iii) Certification by Specialized Agency	Cross-border data transfer is allowed under 4 conditions: (i) Adequacy Decision by the European Commission (EC) (ii) Standard contract with the overseas data handler (iii) Binding Corporate Rules (iv) Industry Code of Conduct	Promote free data flow, especially through preferential trade agreements
Data protection and privacy	Data subject is granted a broad range of rights, which include being informed of data processing, consenting to data processing, withdrawing consent, accessing, modifying, and deleting personal data, seeking compensation in case of misuse or loss of personal data and lodging complaints	Users have the right to be informed and to decide whether to consent to, restrict, or refuse processing; request the overseas recipient to access, copy, amend, supplement and delete their personal data when data is transferred overseas and complain when their right is violated	Data subjects have comprehensive rights including right to information, access, rectification, erasure, restrict processing, data portability, object, automated decision making and lodging a complaint	No comprehensive federal law (but ongoing discussions and proposals) Primarily regulate data on a sectoral basis such as Federal Trade Commission Act for consumer privacy in trade, Gramma-Leach-Bliley Act for the financial sector, etc. State-level privacy laws such as in California and Virginia, etc.

Sources: UNCTAD (2021), Xie et al. (2023), Government's documents.

Data localization

Vietnam, China, and the US prioritize national security when implementing data localization requirements. Vietnam stands out by imposing data localization based on a firm's national origin, unlike China and the US, which adopt a sector-specific and data-specific approach. Decree 53, guiding the implementation of the Law on Cybersecurity, mandates data localization only for domestic enterprises. However, foreign companies in 10 specified sectors may face case-by-case data localization measures if they violate cybersecurity laws related to national security. This categorization eases concerns and pressures from foreign governments and the business community regarding regulatory burdens (USTR, 2021).

In contrast, China and the US have adopted sector-specific and data-specific regulations for data localization. China's Cybersecurity Law (CSL) mandates that critical information infrastructure operators store their data within China.[4] Additionally, data processors handling 14 specific types of important data outlined in the CSL are also required to comply with data localization measures. Conversely, the US has a relatively limited scope of sectors subject to data localization requirements. Notably, stringent data localization policies are in place for defense-related data, necessitating that any cloud service provider catering to the Department of Defense stores the data within the country (UNCTAD, 2021). The EU stands apart as it does not incorporate data localization provisions within its GDPR.

Cross-border data flow

Regarding cross-border data transfer, Vietnam has implemented a more rigid mechanism than China and the EU, characterized by a single mechanism outlined in Decree 13. This mechanism pertains to data processors and controllers handling the personal data of Vietnamese citizens, allowing them to transfer such data outside the country. In compliance with this mechanism, all data handlers must create impact assessment reports on cross-border data transfers and promptly submit them to the Ministry of Public Security (MPS) within 60 days since the the commencement of data processing.[5]

Despite its rigidity, the data transfer mechanism offers considerable flexibility by eliminating the need for prior authorization. Data can be legally transferred out of Vietnam as long as the data processor and controller submit the impact assessment reports, which are subsequently made available to the MPS for inspection. However, it is important to note that the existing regulations grant substantial discretionary powers to the authorities, allowing them to terminate cross-border data transfers if they deem it necessary to safeguard national security.

On the other hand, China and the EU offer various mechanisms for cross-border data transfer, with China implementing stricter regulations. In China, firms are allowed to transfer data outside China under three conditions: (i) Eligible firms are required to conduct a security assessment which is reviewed by the Cyberspace Authority of China (CAC).[6] In situations

[4] Including public communication and information services, transportation, e-government services, national defense, finance, public services, water, and energy sectors

[5] The content requirements of the report can be checked in Section 2 of this report.

[6] A firm considered here falls into one of the following categories: it is a critical infrastructure operator, exports important data, processes the personal information of more than 1 million persons, or it has exported personal

where firms are not eligible for the security assessment, they may still transfer data (i) by signing standard contractual clauses between the data exporter and importer, or (ii) if the Chinese affiliate of a multinational corporation obtains certification from a specialized agency to facilitate data transfer within the same corporation.

Under the GDPR, companies are granted the freedom to choose from four mechanisms for data transfers, including: (i) Adequacy Decisions issued by the European Commission, (ii) Standard Contractual Clauses established between the data exporter and data importer; (iii) Binding Corporate Rules (BCRs), which are internal data protection policies implemented by multinational organizations; and (iv) Industry Code of Conduct, subject to approval by local authorities. Presently, there are no specific compliance requirements in place for cross-border transfers of personal data in the US (UNCTAD, 2021).

Privacy and data protection

Data subjects in Vietnam are granted a set of rights that bear a resemblance to those outlined in the GDPR, one of the earliest and most comprehensive regulations established to safeguard data, and in China's PIPL. Specifically, in Vietnam, data subjects possess rights that include being informed about data processing, providing consent for data processing, withdrawing consent, accessing personal data, modifying personal data, and deleting personal data. In case of mishandling or loss of personal data, users can lodge a complaint to the authority.

Unlike Vietnam, China and the EU, there is no standalone federal data protection framework in the US. Instead, federal laws have been enacted to regulate specific industries such as healthcare, financial data, and communications. Additionally, certain states, such as California and Virginia, have implemented their own data protection regulations.

5. Conclusion

The data governance framework in Vietnam operates under a limited model, wherein data security is closely intertwined with cybersecurity, national interest, and security. To ensure these objectives are met, the Vietnamese government has established laws and regulations that encompass both internal and external safeguards. These measures include data localization requirements, limitations on cross-border data transfers subject to specific conditions, and comprehensive rights granted to data subjects.

However, in comparison to major countries such as the US, the EU, and China, Vietnam faces limitations in imposing stringent data regulations independently. It must consider external pressures from foreign governments with vested business interests in Vietnam, as well as its international obligations stemming from preferential trade agreements concerning data regulations. A notable example is Vietnam's data localization requirement, which is based on

information of more than 100,000 individuals or sensitive personal information of more than 10,000 individuals since January 1 of the previous year.

the origin of companies (domestic vs. foreign) rather than adopting a conventional sector-specific and data-specific approach.

When comparing Vietnam's data regime with the aforementioned countries, it aligns closely with China's limited model, given their similar political regime and economic model. In contrast, data regulations in the EU and the US exhibit relatively less stringency. It is important to acknowledge that irrespective of whether an open or limited model is adopted, governments often justify their data governance practices based on national security concerns. Even in the case of the US, which is generally seen as having a more liberal data regime, data localization requirements have been enforced under the pretext of national security considerations.

REFERENCES

Asian Development Bank (ADB). (2022). The Regional Comprehensive Economic Partnership Agreement: A New Paradigm in Asian Regional Cooperation?. ADB https://www.adb.org/sites/default/files/publication/792516/rcep-agreement-new-paradigm-asian-cooperation.pdf

Burri. M. (2021). Creating Data Flow Rules through Preferential Trade Agreements. Social Science Research Network (SSRN) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3910408

Busch. E. K. (2023). TikTok: Recent Data Privacy and National Security Concerns. Congressional Research Service (CRS) https://crsreports.congress.gov/product/pdf/IN/IN12131

Committee Majority Staff. (2023). Hearing Entitled "TikTok: How Congress Can Safeguard American Data Privacy and Protect Children from Online Harms". House Committee on Energy and Commerce https://d1dth6e84htgma.cloudfront.net/Memo_03_23_2023_Full_Committee_Tik_Tok_Hearing_55e129f043.pdf?updated_at=2023-03-20T21:12:05.159Z

Fefer, R.F., Akhtar, S.I. & Sutherland, M.D. (2021). Digital Trade and U.S. Trade Policy. Congressional Research Service https://sgp.fas.org/crs/misc/R44565.pdf

Fefer, R.F. & Archick, K. (2022). U.S.-EU Trans-Atlantic Data Privacy Framework. Congressional Research Service https://crsreports.congress.gov/product/pdf/IF/IF11613

Ferracane, M.F. & Marel, E. (2021). Regulating Personal Data: Data Models and Digital Services Trade. World Bank Group https://documents1.worldbank.org/curated/en/890741616533448170/pdf/Regulating-Personal-Data-Data-Models-and-Digital-Services-Trade.pdf

Gao, H. S. (2019) "Data Regulation with Chinese Characteristics", SMU Centre for AI & Data Governance Research Paper No. 2019/04; Singapore Management University School of Law Research Paper No. 28/2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3430284

González, J.L., Casalini, F. & Porras, J. (2022). A Preliminary Mapping of Data Localisation Measures. OECD Publishing https://www.oecd-ilibrary.org/docserver/c5ca3fed-en.pdf?expires=1686379173&id=id&accname=guest&checksum=F1AAD4338A7BFCB10CDE1D30258EE379

Jonathan Lim. (2021). Bite the Bullet: The Future of Data Protection Law and Policy in ASEAN. ASEAN Ideas in Progress Series
https://cil.nus.edu.sg/publication/bite-the-bullet-the-future-of-data-protection-law-and-policy-in-asean/

Mark Barnes. (2023). Vietnam's Personal Data Protection Decree: A Quick Guide. Vietnam Briefing
https://www.vietnam-briefing.com/news/vietnams-personal-data-protection-decree-a-quick-guide.html/

Ministry of Industry and Trade (MOIT). (2021). Decree 14 on E-Commerce. Thu vien phap luat
https://thuvienphapluat.vn/van-ban/Thuong-mai/Van-ban-hop-nhat-14-VBHN-BCT-2021-Nghi-dinh-quan-ly-hoat-dong-thuong-mai-dien-tu-496569.aspx

National Assembly. (2007). Law on Information and Technology. Thu vien phap luat
https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Luat-cong-nghe-thong-tin-2006-67-2006-QH11-12987.aspx

National Assembly. (2016). Law on Cyberinformation Security. Thu vien phap luat
https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Luat-an-toan-thong-tin-mang-2015-298365.aspx

National Assembly. (2019). Law on Cybersecurity. Thu vien phap luat
https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Luat-an-ninh-mang-2018-351416.aspx

Nakanishi. T. & Hori. S. (2023). Data Free Flow with Trust: Overcoming Barriers to Cross-Border Data Flows. World Economic Forum
https://www3.weforum.org/docs/WEF_Data_Free_Flow_with_Trust_2022.pdf

To. L. (2021). Chủ quyền không gian mạng: Yêu cầu thời đại và nghĩa vụ quốc gia. CAND Publishing

Trachtenberg, D.M. (2023). Digital Trade and Data Policy: Select Key Issues. Congressional Research Service
https://crsreports.congress.gov/product/pdf/IF/IF12347

United Nations Conference on Trade and Development (UNCTAD). (2016). Data protection regulations and international data flows: Implications for trade and development. UNCTAD
https://unctad.org/publication/data-protection-regulations-and-international-data-flows-implications-trade-and

United Nations Conference on Trade and Development (UNCTAD). (2021). Digital Economy Report 2021: Cross-border data flows and development: For whom the data flow. UNCTAD https://unctad.org/system/files/official-document/der2021_en.pdf

United States Trade Representative (USTR). (2021). 2021 National Trade Estimate Report on Foreign Trade Barriers. USTR https://ustr.gov/sites/default/files/files/reports/2021/2021NTE.pdf

Vietnam's Ministry of Information and Communications (MIC). (2022). Viet Nam has over 72 million Internet users. MIC https://english.mic.gov.vn/Pages/TinTuc/tinchitiet.aspx?tintucid=156626#:~:text=Viet%20Nam%20also%20has%2094.2,that%20there%20are%20over%20564%2C000%20%E2%80%9C

Vietnam's Ministry of Information and Communications (MIC). (2023). Vietnam records best-ever performance in digital economic development. MIC https://english.mic.gov.vn/Pages/TinTuc/tinchitiet.aspx?tintucid=157605#:~:text=The%20contribution%20of%20the%20digital,by%20the%

XIE, Taojun, Jingting LIU, Ulrike SENGSTSCHMID and Yixuan GE. (2023). Navigating Cross-Border Data Transfer Policies: The Case of China. Research Paper #01-2023, Asia Competitiveness Institute Research Paper Series https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4408947

APPENDICES

Appendix 1. Developments of data localization requirement in the EU

Among the four countries under consideration, it is noteworthy that the EU stands apart as it does not incorporate data localization provisions within its General Data Protection Regulation (GDPR). Nevertheless, mounting apprehensions within the EU regarding surveillance practices by the US on the personal data of EU citizens have prompted the European Court of Justice (ECJ) to invalidate two commercial data transfer agreements between the US and the EU. This development has compelled EU policymakers to reconsider the potential implementation of data localization requirements. Notably, EU data protection authorities and stakeholders have voiced support for the notion of mandating that the personal data of EU citizens be exclusively stored within the EU or other approved countries (Fefer & Archick, 2022).

Appendix 2. Cross-border data transfer regulations in the US

The US stands out as an exceptional case regarding regulations governing the transfer of data across borders. Presently, there are no specific compliance requirements in place for cross-border transfers of personal data in the US (UNCTAD, 2021). Nevertheless, efforts have been made to discourage restrictions on data transfer through preferential trade agreements like the TPP, U.S.-Mexico-Canada Agreement, and US-Japan Digital Trade Agreement.

Box 4. Case study: TikTok in the United States

TikTok's background

TikTok, a social media app for creating and sharing short videos, is a subsidiary of ByteDance Ltd., a privately held company based in Beijing, China. With over 150 million users in the United States (US), policymakers in the US have expressed concerns about TikTok's potential privacy and national security risks due to its connections with the People's Republic of China (PRC).

Issues and concerns

On March 23, 2023, during a House Energy and Commerce Committee hearing, TikTok CEO Shou Zi Chew addressed concerns related to data privacy, national security, and children's online safety.

Consumer Privacy and Data Security. Critics are concerned that TikTok, being owned by a Chinese technology company, is subject to China's cybersecurity and data security laws. These laws grant the government access to data and impose requirements for data localization and processing in China.

Content Manipulation. National security officials are concerned that TikTok's content moderation and recommendation algorithms may be influenced by the PRC, leading to the promotion of misinformation, propaganda, or censorship of content for US citizens.

Responses to TikTok's potential threats

In response to concerns about TikTok's potential threats to US national security, bans have been imposed by the federal and state governments. Executive agency devices are prohibited from accessing TikTok and other ByteDance services, and some or all state-owned devices are also affected. Additionally, the Biden Administration has called for the divestiture of TikTok from the PRC.

Trends in Legislation

Recently, the US Congress has proposed legislation to safeguard the personal data of US citizens. These proposals include comprehensive federal privacy laws like the American Data Privacy and Protection Act, as well as bills aimed at regulating the export of US data to other countries, such as the Protecting Americans' Data from Foreign Surveillance Bill.

Source: US Congressional Research Service, US House Committee on Energy and Commerce.

However, the TikTok incident has prompted US lawmakers to contemplate the implementation of data protection measures on a federal scale (Box 4). With a substantial increase in users within the US and concerns regarding TikTok's alleged national security risks due to its data security and connections to the People's Republic of China, legislators have introduced bills proposing restrictions on cross-border data transfers (Mulligan & Brannon, 2023).

One such bill is the Protecting Americans' Data from Foreign Surveillance Bill, which was introduced in 2022. This bill aims to establish export controls on the personal data of US citizens and individuals residing in the US. The intention is to prevent foreign governments from exploiting this data to compromise US national security, with the threshold for regulation set by the Department of Commerce. Specifically, the proposed threshold for regulating the transfer of personal data to restricted countries would be not less than 10,000 covered individuals and not more than 1,000,000 covered individuals during a year (Wyden, 2022).