STUDIA JURIDICA ET POLITICA JAURINENSIA
VOL. 12, NO. 2, 2025, 123–142.
DOI: 10.71100/STUDIA.2025.2.8

DATA LOCALIZATION, INTERNATIONAL LAW PERSPECTIVE

ALI, SHAREEF SANAR[1]

ABSTRACT

Although the core principles of the General Agreement on Trade in Services (GATS) can extend the agreement to the movement of data, thereby enhancing the effectiveness of GATS in the digital age, there is very little to prevent governments from implementing wide data localisation measures, as GATS provides broad exceptions that create leeway for circumventing these obligations. Additionally, the ambiguity surrounding internet technology has given governments more justification. After all, how could anyone challenge these policies when technology and intelligent services themselves were once incapable of detecting what Edward Snowden later exposed? In response to these uncertainties, and the existing security exceptions in GATS, countries continue to invent new data localisation measures through different approaches. China forbids data transfers by default, only allowing them as exceptions, and emphasises national security with ambiguous discretionary limits. The GDPR limits transfers from outside the EU in order to balance privacy and trade but provides exceptions. The USA, without a unified federal legislative framework, has focused localization on areas such as taxation and defence, motivated mostly by national security. Given these dynamics, and the sensitivity of national security, the author argues that greater emphasis should be placed on reactivating the role of WTO panels and, at the very least, establishing broad boundaries for what constitutes security, even if the concept itself is difficult to define precisely.

KEYWORDS Data protection, data localization, data flow, international trade law, trade barriers, WTO panels

1. Introduction

The emergence of the Internet and advances in technology have had a great impact on international trade and the global economy. Personal data is often described as the fuel of the internet and the new currency of the digital realm (National Board of Trade, 2014, p. 10). Almost half of international trade in

[1]PhD Student and Lecturer at Károli Gáspár University of the Reformed Church in Hungary, Doctoral School of Law and Political Sciences, Budapest, Hungary.

services now relies on information and communications technology (ICT) (National Board of Trade, 2014, p. 9). At first, this development was expected to push the international community toward reducing trade barriers. However, data localisation measures have undermined this expectation by restricting data transfers. Many countries have adopted measures that make the transfer of personal data across borders difficult, justifying them on the grounds of privacy and security, thereby creating significant obstacles to data exports (Chander & Le, 2014, p. 8). The unprecedented development of technologies, products, and services today has relied heavily on the free flow of data across borders. The operation, innovation, and maintenance of competitiveness of companies in global markets all rely on data movement. Data localisation practices fragment the World Wide Web, which was initially intended to enable global information trading (Chander & Le, 2014, p. 8).

While many commentators suggest that data localisation falls within the scope of GATS Mode 1 (cross-border trade) (Abe, 2021, p. 11; Tseng, 2024), the central issue is not whether such measures are covered by the GATS. This is because, on the one hand, countries often justify data localisation measures on the grounds of protecting national security and citizens' privacy, rather than asserting their permissibility under the GATS. On the other hand, the GATS explicitly provides for privacy exceptions, thus ensuring that obligations under the agreement do not, by their nature, preclude the implementation of data localisation measures.

The problem addressed in this study lies in the fact that there is currently nothing preventing countries from adopting data localisation measures. This stems from the complexity of the internet and the sensitivity of modern technologies, which prompt countries to take a precautionary approach. It is possible for governments to believe that they were only able to learn about certain spying activities after the Edward Snowden leaks, suggesting that even with the advanced technology they have, they were unable to detect these activities on their own. This reinforces their belief that enhanced data surveillance through localisation is essential for national security.

On the other hand, while the General Agreement on Trade in Services (GATS) establishes important principles aimed at promoting free trade, its exceptions – particularly security exceptions – may undermine these principles. A key issue is the self-judging nature of the security exception, which is enshrined in the agreement's language. Some countries support this interpretation, while others oppose it, sparking ongoing international controversy. This disagreement has extended to the interpretation of the exception by WTO panels, which have adopted inconsistent approaches. Ultimately, this contributed to the suspension of the WTO panels' work since 2019.

However, the crucial question is the fairness of data localisation measures and their ability to effectively balance the protection of international trade interests, national security, and personal data protection. To address this issue, the study poses several key questions: What is data localisation, and how do different jurisdictions address it? To what extent does the GATS restrict states' authority to enact such measures? And how successful is the GATS in challenging or limiting these measures?

To explore these questions, the study will examine three major jurisdictions – the United States, China, and the European Union – which together account for nearly 90% of global trade. Accordingly, the study is divided into two main sections. The first section will explain the concept of data localisation, analyse how each of the three jurisdictions addresses it, and assess its impact on international trade. The second section will focus on the GATS agreement – how it treats cross-border data transfers, how its core principles may limit data localisation measures, the extent of its effectiveness in curbing such measures, and the role of WTO panel rulings in this context.

2. THE CONCEPT OF DATA LOCALIZATION AND ITS IMPACT ON INTERNATIONAL TRADE

2.1. The concept of Data Localization

It is not easy to define this term, as it lacks a universally accepted definition (Del Giovane et al., 2023, p. 5), and its meaning varies depending on the context (Whorra, 2022, p. 44). However, it may be understood as a mandatory legal or administrative (OECD, 2020, p. 8) requirement, or the practice of storing or processing (Fahey, 2023, p. 505) data within the territorial borders of a country. In other words, it involves keeping data locally to protect against the leakage of personal information (Singh, 2022, p. 496).

There is a controversy about what exactly constitutes data localisation: some believe that it includes implicit measures such as limitations on cross-border data flows, while others emphasize explicit regulations that directly dictate where and how data is stored or processed within a jurisdiction (Del Giovane et al., 2023, p. 5).

In the wake of Edward Snowden's intelligence revelations, many governments have considered "data localisation" laws that restrict the storage, transfer, and processing of digital data to specific locations, jurisdictions, or companies (Hill, 2014). Many countries, developed and developing (Hodson, 2019, p. 580), have adopted data localisation laws (Lu, 2024, p. 183). By early 2023, nearly 100 data localisation measures had been implemented across 40 countries, with over half of them introduced since 2015 (Del Giovane et al., 2023, p. 3). These regulations

take various forms and sizes. In terms of data type, data localisation measures can be classified into three main groups: the first is blanket localization, which requires all types of personal data to be stored within the country; the second is specific localisation, which applies to specific categories of personal data and specific organizations and mandates data be stored locally (Fraser, 2016, p. 360); and the third is combined localisation, which focuses on specific categories of personal data without requiring local storage. Instead, the focus is on ensuring that the processing of data is carried out in accordance with legal requirements (Singh, 2022, p. 496). In terms of regulatory frameworks, there are various categories of legislation, ranging from outright bans on the transfer of all types of data (Devane, 2022) to targeted restrictions, which apply only to transfers of data in specific sectors, rather than to all data (Satori Cyber, 2024).

2.2. In Practice

The United States, the European Union, and China, which collectively control 90% of world trade (Kyger, 2024), share many commonalities in regulating data transfer, but there are also fundamental differences. Each has imposed restrictions on data transfers, albeit of varying nature and scope.

2.2.1. China

With the introduction of several laws and regulations, privacy legislation in China has become more complex. These regulatory frameworks include strict guidelines regarding the transfer of personal data stored in China to foreign entities (Tang, 2021). While privacy rights are addressed, the main goal of restricting cross-border data flow is to protect national security interests (DSL, arts. 10, 25; ODTSAM, arts. 1, 8; NDSM Regulation, art. 1)[2]. Although the reasons behind LinkedIn's and Yahoo's 2021 withdrawals from China remain unclear, their exits demonstrate the difficulties of adhering to the country's strict data localisation regulations (Lu, 2024, p. 183).

Unlike the EU, China doesn't have a unified data protection framework. Instead, its personal information protection system is based on three primary laws: The Personal Information Protection Law (PIPL), the Cybersecurity Law (CSL), and the Data Security Law (DSL) (DLA Piper, 2024, p. 2). Additionally, there are specific laws regulating data transfers, which provide detailed guidelines and

[2] See, for example: The Data Security Law, in Article 25, implements export controls for certain types of data to safeguard national security, while Article 10 prohibits the transmission or processing of data that endangers national security or public interests. Data Security Law of the PRC (effective 10 June 2021). In addition, Article 1 of the Outbound Data Transfer Security Assessment Measures provides: *"In order to regulate outbound data transfer activities […] safeguard national security […] these Measures are formulated."* Article 8 evaluates the potential risks associated with outbound data transfers, focusing on their impact on national security, public interest, and the legal rights and interests of individuals and organizations. Outbound Data Transfer Security Assessment Measures (effective 1 September 2022). See also Article 1 of The Regulation on Network Data Security Management (China, adopted at the 40th executive meeting of the State Council, 30 August 2024, effective 1 January 2025).

restrictions, such as Article 5 of the Regulations on Network Data Security Management (NDSM Regulation), the Regulations on the Security Protection of Critical Information Infrastructure (CII Regulations), and the measures adopted by the State Administration for Market Regulation and National Standardization Administration (GB/T 43697-2024). Furthermore, various provisions in different Chinese laws impose restrictions on the transfer of data outside China[3].

Operators of critical information infrastructure in China are required by Article 37 of the Cybersecurity Law to store sensitive or personal data within mainland China. A security assessment must be conducted in accordance with applicable laws and regulations if data must be moved outside the country for business purposes (CSL).

Conditions for transferring personal data outside of China are imposed by Article 38 of the PIPL. Personal information processors are required to sign a standard contract, pass a security assessment, obtain a personal information protection certificate, or adhere to other legal or regulatory provisions specified by the state cybersecurity authority.

Article 4 of the Outbound Data Transfer Security Assessment Measures mandates that data handlers apply for an outbound data transfer security assessment if they provide important data abroad, if a critical information infrastructure operator or data operator has sent more than 1 million people's personal information abroad, or if they have sent over 100,000 people's personal information or the sensitive personal information of 10,000 people since 1 January of the previous year. In addition, a security assessment is necessary in other circumstances as determined by the State Cybersecurity and Information Department (ODTSAM). This gives the department discretionary power to decide standards without clear boundaries and leaves the list vulnerable to further restrictions. In addition, the security assessment measures do not explain how the personal data thresholds (1 million, 100,000, and 10,000 individuals) are calculated. It is not obvious whether these thresholds are applicable to all types of personal data processed by an entity, regardless of information systems, business functions, or data subjects' categories (Yin et al., 2022).

2.2.2. European Union

In Europe, both the Data Protection Directive, which preceded the General Data Protection Regulation (GDPR), and the GDPR contain rules forbidding limitations on data flows among Member States, ensuring free data transfer within the EU

[3] See, for example: Article 24 of Order of the State Council of the People's Republic of China No. 631: Regulation on the Administration of the Credit Investigation Industry (adopted at the 228th executive meeting of the State Council on 26 December 2012, effective from 15 March 2013); Articles 28 and 57 of Standing Committee of the National People's Congress: PRC Law on the Protection of State Secrets (promulgated on 27 February 2024). Article 6 of Notice of the People's Bank of China on Protecting Personal Financial Information by Banking Financial Institutions (last amended in 2011).

and EEA. For non-EU countries, however, both the Directive and the GDPR have a protective and restrictive strategy, which restricts data transfer to protect privacy. The GDPR, which replaced the Directive and refined it with a more uniform and robust system, maintains the same fundamental principle of restricting data flow outside these zones. It defines its subject matter and objectives in terms of two main points: respect for personal data and recognition of the necessity of data transfer for international trade and cooperation. However, realizing this balance is not always an easy task for the EU. The EU anticipated these difficulties early on and has established flexibility within its rules to ensure that data protection does not unduly hinder economic activities or international data transfer. This flexibility is found in Article 52(2) of the EU Charter of Fundamental Rights, which provides that the rights enshrined in the Charter and outlined in the Treaties must be exercised in accordance with the terms and within the restrictions specified in those Treaties (CFR).

The GDPR offers several acceptable grounds for lawful international data flow. Article 45 (1) and (2) provides that the transfer of personal information to a third nation is permitted if the European Commission has determined that the country offers a sufficient degree of protection. The Commission evaluates this adequacy by taking into consideration many factors such as the rule of law, supervisory authorities, and international commitments. As an alternative, Article 46 provides for suitable protection such as binding corporate rules[4], standard contractual clauses (European Commission, 2021), codes of conduct, or certifications, so long as they guarantee that data subjects have enforceable rights and legal recourse.

For non-personal information, Art. 37 of the Chinese Cybersecurity Law requires operators of critical information infrastructure in China to store within mainland China any important data that they collect or generate in the course of their operations. Where it is necessary to provide such data overseas for trade purposes, the operator must first undergo a security assessment in accordance with applicable laws and regulations. Under Article 31, critical information infrastructure covers sectors such as public communications, finance, and public services, whose disruption or data leakage could threaten national security or public welfare (CSL).

Certain cross-border activities that do not involve personal information or critical data, such as "international trade, cross-border transportation, academic cooperation, cross-border production and manufacturing, and cross-border marketing," are exempt from Article 3 of the Regulations on Promoting and Regulating Cross-Border Data Flow. The EU, on the other hand, approaches non-

[4] Article 4(20) of the GDPR defines "binding corporate rules" as rules that apply to transfers, or sets of transfers, of personal data to a controller or processor in one or more third countries within a group of undertakings or enterprises engaged in a joint economic activity.

personal data differently, with a more expansive framework and more stringent regulations. The European Data Governance Act (DGA), the Data Act (DA), and the forthcoming European Health Data Space (Inside Privacy, 2022) impose restrictions on the transfer of non-personal data outside the EU. Although it might seem that the main goal of these restrictions is to safeguard non-personal data, they also seek to prevent people from being re-identified using that information (Van Quathem & Oberschelp de Meneses, 2024).

2.3. United States

The USA does not have a comprehensive data protection regulation that is comparable to the GDPR in Europe. Instead, it handles data privacy through a patchwork of sector-specific and state laws.

The U.S. expresses its policies and policy position on data localisation through international governance organizations and trade agreements, such as the United States-Mexico-Canada Agreement, which forbids data localisation and promotes the free movement of data among the member countries (Global Regulatory Insights, 2025). However, certain laws pertaining to residency or data localisation may mandate that personal data be stored within the country (Global Regulatory Insights, 2025). Several data localisation requirements have been proposed or implemented, primarily centered on public procurement (Cory, 2017, p. 30). Recently, the U.S. pushed to remove financial services data from the Trans-Pacific Partnership's regulations that barred countries from imposing barriers to data transfer. However, after the deal was concluded, the U.S. sought to limit the extent of this exemption through bilateral discussions and provisions in ongoing Trade in Services negotiations (Cory, 2017, p. 30). Data localisation requirements in the United States are affected by several factors, including national security regulations, and the U.S. approach to data localisation aims to balance national security and data protection with the free transfer of data for economic and security reasons (Global Regulatory Insights, 2025). Biden's executive order cites national security, foreign policy, privacy protections, and other human rights and freedoms as justifications for its issuance (EO 14117).

Data localisation requirements in the United States are governed by both federal- and state-level laws, each emphasizing the protection of sensitive information within U.S. jurisdictional boundaries. At the federal level, Internal Revenue Service Publication 1075 (Internal Revenue Service, 2021, p. 57) mandates that Federal Tax Information (FTI) must be accessed, processed, stored, and transmitted within the United States, including its territories, embassies, and military installations. This regulation explicitly prohibits foreign remote maintenance, call centres, or help desks from handling FTI. Similarly, the

Defense Acquisition Regulations System (239.7602–2) (DFARS Rule, 51739) requires cloud computing service providers to keep all federal data within the 50 states, the District of Columbia, or outlying U.S. areas, unless specifically permitted by a designated authority. This aligns with the City of Los Angeles' agreement with Google, which states that email and Google Message Discovery data must stay in the continental United States, as outlined in the Statement of Work (Appendix B, Section 1.1.10.4) (City of Los Angeles, 2009).

At the state level, a number of bills filed in the early 2000s sought to impose similar restrictions, particularly targeting call centres and the cross-border flow of personal data. For example, Missouri House Bill No. 1497 (2004) (National Foundation for American Policy, 2004) forbids state contracts with centres located abroad and bans the transfer of financial, credit, or identifying information to foreign nations without specific written consent (Section 1, Subsection 3). Similar clauses are found in Kansas House Bill No. 2810 (2004), Washington House Bill No. 3186 (2004), and Tennessee Senate Bill No. 3492 (2004), all of which limit the use of overseas contact centres for state contracts and require operators to reveal their location upon request. Ohio House Bill No. 459 (2004) also sought to forbid state contract work from being done outside of the United States and required consumer authorization for data transfers abroad (National Foundation for American Policy, 2004).

Section 202.301 of Biden's order forbids the transfer of covered data transactions – involving access to government-related data or large amounts of sensitive personal data – to covered individuals or countries of concern (Department of Justice, 2024).

In sum, China adopts a state-centric, security-driven paradigm characterized by complex, case-by-case security evaluations, volume-based thresholds, and discretionary enforcement. This model often leads to regulatory opacity and compliance difficulties – particularly for foreign firms. In contrast, the EU adheres to a harmonised, rights-based framework under the GDPR, applying uniform standards based on fundamental rights, with cross-border transfers allowed through mechanisms including standard contractual clauses and adequacy determinations. Unlike China's flexible exclusions for smaller-scale data flows and geographic carve-outs like free trade zones, the EU maintains uniformity regardless of data amount or company size. The United States, meanwhile, lacks a single data protection law and takes a more practical, sectoral, and trade-oriented approach, giving national security priority in certain areas but largely supporting data mobility, especially through international agreements. Despite variations in form and degree, data localisation measures are increasingly considered obstacles to the global economic system. This raises the question of the legality of such actions under international trade law: how much does

international law regulate this area, and to what extent does it permit such practices?

3. DATA LOCALIZATION UNDER GATS

When the General Agreement on Trade in Services (GATS) was created in 1994, the Internet was still in its infancy, so it is not surprising that the GATS does not directly address digital trade obstacles (Hodson, 2019, p. 582). However, such flows may still be covered by Article I of GATS under 'mode of supply 1' (cross-border trade) when data transfers enable the provision of services across borders (Yakovleva, 2020, p. 893). The provision of services through Mode 1 does not require the physical presence of a supplier from one Member State in another; therefore, under WTO jurisprudence, this mode also encompasses trade in digital services. Cross-border data transfers are essential to enabling services under Mode 1 commitments, such as online consultancy and e-commerce (World Trade Organization, 2004, para. 7.45). Additionally, Mode 3, the supply of a service "by a service supplier of one Member, through commercial presence in the territory of any other Member", can also be affected by data transfer restrictions. For instance, if a foreign business sets up a local subsidiary to offer retail services in a host nation but faces restrictions on transferring customer data for analysis back to its home country, this restriction would impact its capacity to provide services (Abe, 2021, p. 12).

Furthermore, nations do not challenge the applicability of the GATS to digital data; instead, they affirm their commitment to facilitating data flows in their legislation (PRRCDF Regulation, art. 1; ODTSAM, art. 1; DSL, art. 1; EO 14117, sec. 1), indicating their approval of the application of the GATS to digital data transfers. Therefore, the matter of data transfers being covered by the GATS can be considered settled.

This leads to the next stage: examining to what extent data localisation contravenes fundamental WTO principles such as most-favoured-nation treatment and market access, among others, which were initially designed to encourage free trade and remove barriers to economic development.

3.1. The core principles of GATS

3.1.1. Most-Favored-Nation Treatment (MFN)

According to GATS Article II, WTO Members shall treat comparable services and service providers equally, regardless of their country of origin. Even if a country has not made specific commitments in the service sector, it is nevertheless required to abide by the most-favoured-nation (MFN) obligation, which applies to all measures under the agreement. A data localisation measure could violate

Article II:1 by causing unjustified discrimination if it unfairly targets or favours certain countries.

This raises the question of whether the MFN principle is violated when service providers are differentiated based on a GDPR adequacy decision. Due to significant differences in data protection standards, services and service providers from nations with different degrees of data protection may not be deemed "like" under the GDPR. Therefore, the 'likeness' requirement of the MFN principle may not be violated if an adequacy decision is grounded solely in the level of data protection offered by a country rather than in the country of origin itself (Yakovleva, 2018, p. 491). According to the Appellate Body report in Argentina – Financial Services, in assessing 'likeness' under the MFN principle and data protection adequacy decisions, it is crucial to evaluate whether the services and suppliers are in a competitive relationship. This may involve adapting criteria from goods trade, such as the nature and quality of services and consumer perceptions, to suit the specifics of services trade (World Trade Organization, 2016).

3.1.2. Domestic Regulation

Paragraph 5 of Article VI of the GATS aims to prevent unnecessary trade barriers in services by forbidding the application of licensing and qualification requirements and technical standards that invalidate or undermine particular commitments. These requirements must meet the standards of objectivity, transparency, and minimal burden. Therefore, if data localisation laws fail to satisfy these criteria, they may conflict with the obligations under Article VI.

3.1.3. Market access

Article XVI(2) (World Trade Organization, 2025) provides that in sectors where market-access commitments are undertaken, Member States are not permitted to impose limitations on the number of service suppliers or limitations on the total number of service operations or the total quantity of service output (e.g. quotas or economic needs tests), unless otherwise specified in their Schedule. According to the US–Gambling case, the Appellate Body determined that banning the online supply of gambling and betting services constitutes a "zero quota", violating GATS Articles XVI:2(a) and (c) (World Trade Organization, 2005, paras. 238, 251). This reasoning could similarly apply to limitations on the cross-border flow of entire categories of data, particularly if these categories align with service sectors where a country has made unqualified market-access commitments (Mitchell & Hepburn, 2017).

3.1.4. National Treatment

According to Article XVII of the GATS, foreign services and service providers are treated no less favorably than domestic "like" services and providers, but only in sectors where specific commitments are listed in their Schedule. This obligation can apply to Mode 3 (commercial presence), where the service supplier operates in another Member's territory. Data localisation measures, such as requiring domestic data storage or facility installation, may disproportionately burden foreign providers by increasing their costs, thereby harming competition between foreign and domestic suppliers. Such measures could violate national treatment obligations.

The EU stated in the Council for Trade in Services that *"foreign companies operating in China could find themselves in a de facto less competitive situation compared to domestic operators"* because of the Chinese cybersecurity law. This statement seems to be based on the EU's perception that the Chinese law will likely breach national treatment obligations (Abe, 2021, p. 17).

While GATS principles limit governments' power to legislate data localisation measures and potentially reduce their impact, the agreement's exceptions, specifically security exceptions, effectively give countries leeway to circumvent these obligations. Although panels have worked to narrow the interpretation and the scope of these exceptions, countries' national security concerns continue to challenge the maintenance of these principles, largely due to the agreement's self-judging language, which allows Members discretion in determining their security interests. Additionally, all these principles – with the exception of the MFN principle – require specific obligations on the part of states; otherwise, they are unenforceable, further limiting their applicability.

The GATS provides for general exceptions (Article XIV) and security exceptions (Article XIV bis) to limit trade. General exceptions require an objective analysis to prove that the challenged measure was necessary and to assess whether less restrictive alternatives were available. In contrast, security exceptions do not involve evaluating alternatives but focus on whether a security threat existed and whether the measure was proportional (Bahri, 2020, p. 337).

In US – Gambling, the Appellate Body found that GATS Article XIV parallels GATT Article XX exceptions, making GATT Article XX jurisprudence relevant for the analysis of GATS Article XIV (World Trade Organization, 2005, para. 291)

3.2. Exceptions

3.2.1. General Exceptions

According to Article XIV, on the condition that they don't unjustly discriminate between countries with comparable circumstances or create disguised trade restrictions, the following actions are allowed:

a. necessary to protect public morals or to maintain public order;

   The EU–Energy Package panel pointed out two elements that a party invoking this subparagraph had to prove, one of which is that the measure must be one intended and required to protect public morals or to maintain public order (World Trade Organization, 2018, para. 7.230). In another case, the Panel argued that the content of these ideas for Members might change throughout time and space based on a range of circumstances, including prevailing social, cultural, and religious values. More specifically, Members ought to have some scope to define and apply for themselves the concepts of public morals and public order in their own regions, according to their own systems and scales of values (World Trade Organization, 2004, para. 6.461).

b. necessary to protect human, animal, or plant life or health;

c. necessary for compliance with WTO-consistent laws and regulations, including those about:
   - preventing fraud and dealing with contract defaults
   - protecting personal data privacy and confidentiality
   - safety.

The Argentina–Financial Services Panel assessed 'necessity' under Article XIV(c) GATS by considering three factors:

a. the importance of the objective pursued,

b. the measure's contribution to that objective,

c. the measure's trade-restrictiveness.

It then held that a comparison between the measure and possible alternatives must also be undertaken (World Trade Organization, 2015, para. 7.661).

According to the US–Shrimp (Thailand) Panel, for an Article XX(d) GATT defence, a Member must:

- identify which laws or regulations the measure aims to enforce
- prove that these laws or regulations are WTO-consistent
- show that the measure is designed to secure their compliance (World Trade Organization, 2009, para. 7.514; World Trade Organization, 2008, para.

7.174; World Trade Organization, 2015, paras. 7.595–7.596). Moreover, the provided list is non-exhaustive (World Trade Organization, 2004, para. 6.540).

According to the Argentina–Financial Services Panel, in order to provide a proper weighing and balancing, detailed assessments are essential. It emphasized that a 'necessity' analysis requires evaluating the degree (qualitative and quantitative) of the measure's contribution to the objective, not just if it contributes, and evaluating the level of trade-restrictiveness, not just if trade is restricted (World Trade Organization, 2016, para. 6.234).

The Appellate Body in Korea–Beef stressed the importance of weighing and balancing to ascertain whether alternative measures exist that are consistent or less WTO-inconsistent while still accomplishing the policy purpose, thereby ensuring minimal deviation from WTO rules (World Trade Organization, 2000, para. 165).

3.2.2. Security Exceptions

According to Article XIV bis, this Agreement does not:

a. require Members to furnish any information which they consider contrary to their essential security interests; or

b. prevent Members from taking any action which they consider necessary to protect their essential security interests:
   - relating to services directly or indirectly supplying military establishments;
   - relating to fissionable and fusionable materials or materials derived from them; or
   - taken in time of war or other emergency in international relations.

The phrase "it considers" gives Members discretion to determine what information or actions are necessary for their security interests. This self-judging language creates controversy between countries supporting broad national discretion and those opposing the potential abuse of security exceptions.

On the occasion of Portugal's 1961 accession, Ghana justified its boycott of Portuguese goods under Article XXI(b)(iii), arguing that each Member is the "sole judge" of its essential security interests, and that security threats can be both potential and actual. In the 1982 Geneva discussions on Article XXI GATT invocations, Members expressed opposing views. Uruguay, Colombia, Poland, Argentina, and Brazil emphasized the need to justify security measures, arguing that measures against Argentina lacked legal and economic basis and could undermine GATT principles and international cooperation. In contrast, Australia, the EEC, the US, and Canada maintained that Article XXI measures required

neither justification nor notification, citing inherent rights and historical precedent, and supported the self-judging nature of security concerns. They asserted the Members' sovereign right to determine necessary actions without external approval, with the US specifically noting that this applies in "times of international crisis" (General Agreement on Tariffs and Trade, 1982, pp. 6–12). While this US position appears to restrict the wide interpretation of security interests to crisis times, the US has demonstrated an even broader interpretation of security interests in other cases.

In the US–Nicaragua case, the US emphasized that Article XXI leaves each Member to judge for itself the necessary actions for protecting its essential security interests, arguing that GATT, as a trade organization, had no competence to approve or disapprove such judgments. The European Communities, Canada, Australia, Portugal, Iceland, Norway, and Finland supported this broad self-judging interpretation. However, Nicaragua, Cuba, India, Peru, Argentina, Brazil, Spain, and Czechoslovakia opposed this view, arguing that it undermines GATT principles and requires accountability to prevent political abuse (GATT Council, 1985, pp. 2–16).

The Panel's approach to Article XXI has evolved over time. In the Nicaragua case, despite Nicaragua's international law arguments supported by ICJ and UN Security Council decisions, the Panel declined to recommend lifting the embargo, citing its limited mandate in assessing the validity or motivation of national security measures (General Agreement on Tariffs and Trade, 1986, para. 5.15).

However, a shift occurred in Russia – Measures Concerning Traffic in Transit, where the Panel held that while states can define their essential security interests, this must be done in good faith, and affirmed its jurisdiction to review such measures (World Trade Organization, 2019, paras. 7.101–7.102).

In United States – Certain Measures on Steel and Aluminum Products, the Panel explicitly rejected the US argument that the phrase "which it considers" in Article XXI(b) makes the subparagraphs self-judging (World Trade Organization, 2022, para. 7.163).

FTAs are currently the only agreements with binding rules against data localization. Due to political reluctance and lack of consensus, it remains uncertain whether GATS will explicitly classify data localization as trade-restrictive, whether through amendment or legal interpretation. Even within plurilateral negotiations, agreement on this issue is uncertain. As a result, FTAs are expected to shape data governance in the foreseeable future (Ikigai Law, 2020).

3.2.3. Free Trade Agreements (FTI)

While FTAs prohibit requiring a covered person to use or locate computing facilities in a Party's territory as a condition for conducting business, they include broad exceptions for security measures. For example, the United States-Mexico-Canada Agreement (USMCA) explicitly prohibits data localization in Article 19.12 but allows exceptions under Article 32.2 for essential security interests and international peace and security. Similarly, Article 14.13.2 of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) prohibits countries from forcing businesses to store data or locate computing facilities within their borders as a requirement for doing business there. However, countries can depart from this rule where this is necessary to achieve a "legitimate public policy objective", provided that the measure is not discriminatory or used to disguisedly restrict trade, and that the restrictions are not more severe than necessary to achieve the policy goal. Article 29.1.3 adopts paragraphs (a), (b), and (c) of Article XIV of GATS, and Article 29.2 contains a security exception with very similar terms to Article XIV bis.

The ambiguous language in trade agreements regarding exceptions, particularly security exceptions, was not coincidental but rather a deliberate choice to create a kind of "soft law", allowing flexibility in interpretation and making the agreement more acceptable than no law at all. While panels have significantly contributed to broadening the interpretation of principles and narrowing exceptions, the results have not been entirely satisfactory. Many countries continue to view security concerns as purely domestic matters beyond external review, asserting sole authority to evaluate their security interests. This fundamental tension has led to the current crisis in the WTO dispute settlement system, with the Appellate Body having been non-functional since December 2019 due to the US blocking new appointments since 2016, leading to unresolved appeals and ineffective panel reports (Kerstens & Reinsch, 2023). The European Parliament's serious concerns about this paralysis reflect broader fears for the rules-based trading system (European Parliament, 2019), especially as the US increasingly invokes security exceptions to justify various trade measures while criticizing panels for allegedly overstepping their authority in interpreting these provisions, claiming that such interpretation infringes on national sovereignty and regulatory rights (Kerstens & Reinsch, 2023).

The tension between the interests of individual states and those of the international community, as well as the broader conflict between international law and state sovereignty, is a well-documented phenomenon. This tension is particularly pronounced in the domain of technology and the internet, which inherently transcend national borders. In the aftermath of Edward Snowden's disclosures, many states have reassessed their legal frameworks and

implemented more stringent data protection measures, reflecting a growing concern over digital sovereignty and security.

Hypothetically, if countries only became aware of certain espionage activities following such revelations, it raises the question of how many undisclosed espionage activities might be ongoing, awaiting similar exposure. This situation suggests that technology, in its current state, may be insufficiently robust to detect or predict the capabilities of other technologies. Consequently, it becomes challenging to question the measures states undertake to safeguard their "citizens' privacy" and "national security" in a manner they deem appropriate, especially when there are grounds for that in GATT and GATS.

Governments may see or claim several benefits and justifications for implementing such policies. These include enhancing national security, supporting local economies, protecting human rights (Lu, 2024, p. 184), reducing the risk of breaches and unauthorized access, and strengthening cybersecurity by enabling quicker responses to security incidents (Kiteworks, 2025). The transfer of data across borders raises concerns about the potential leakage of personal information, especially to foreign governments or organizations (Singh, 2022, p. 497). Another reason for data localization is the fear of foreign digital colonization, as countries fear over-reliance on powerful multinational tech companies, especially those from large countries like the United States (Lu, 2024, p. 183). Additionally, it aids law enforcement by ensuring easier access to information for investigations and cybercrime prevention (Bowman, 2017). Therefore, governments must either implement legal interventions or, as Domingo Guerra, co-founder of Appthority, aptly asserts, *"The only way to really make anything that is NSA-proof is to not have it connect to the Internet"* (Swartz, 2014).

Despite the criticisms, the arguments against data localization often lack robust evidence that could persuade governments to change course. Countries are unlikely to sacrifice their national security, economic interests, or citizens' privacy for measures that do not guarantee complete protection. Consequently, they are likely to continue enforcing data localization laws, especially when there are no concrete international rules to prevent them.

Therefore, additional barriers to data flow, in various new forms, are expected in the future. Countries are leaning towards more decentralized, narrow geographical free trade agreements, which allow them to pick and choose among countries those they regard as trustworthy. Examples include different free trade agreements, or even laws excluding certain countries from data access, such as Biden's executive order, and most concerningly, the possibility of establishing new networks besides the international one. In their paper, Anupam Chander and Owen B. Lee argue that governments around the world

are increasingly asserting control over the World Wide Web, thereby fragmenting it. For example, Iran aims to create an internet free of Western influence and dissent, while Australia restricts the export of health data. Similarly, South Korea requires that map data be stored locally, and Vietnam requires local copies of all Vietnamese data. These measures are akin to the creation of "Schengen data zones," effectively blocking global services. The authors compare this trend to the non-tariff barriers of the last century, which have now resurfaced as digital firewalls blocking international services (Chander & Le, 2014, p. 1).

4. Conclusion

The different strategies used by the US, EU, and China – which together account for 90% of world trade – clearly reflect the difficulties surrounding data localization. Chinese legislation, such as the PIPL and the CSL, forbids data transfers by default, only allowing them as exceptions, and emphasizing national security with ambiguous discretionary limits. The GDPR limits transfers from outside the EU in order to balance privacy and trade, but provides exceptions, such as adequacy decisions, and evaluates nations collectively rather than individual entities, promoting a simpler and more consistent procedure compared to China's intricate operator-specific rules. The United States, without a unified federal legislative framework, blends free-flow promotion in trade agreements like the USMCA with focused localization in areas such as taxation and defense, motivated by national security concerns and public procurement.

Although data localization is not mentioned in GATS, it contains enough provisions to cover data localization concerns, and countries' recognition of the importance of the free flow of data in their laws is clear evidence that data is covered by GATS. GATS does contain numerous principles prohibiting barriers to trade and promoting free commerce among countries for the sake of economic growth. However, it has enough exceptions to pave the way for the adoption of data localization strategies. While these exceptions are necessary to safeguard important societal interests, such as privacy, national security, and crime prevention, the desire of nations to keep national security matters entirely internal, alongside the self-judging language expressed by GATS, renders core GATS principles ineffective. Although panels play a great role in expanding the meaning and application of these principles and narrowing exceptions, the panels themselves have not been consistent, as they have adopted varying stances in different situations. Moreover, the panels have been paralysed since 2019 due to certain countries' persistent affirmation of the self-judging nature of the security exceptions.

These concerns are not unfounded. Without Snowden's revelations, far more sensitive information could have remained unknown yet accessible to foreign authorities. On top of that, the decades-old GATS framework may not fully serve the interests of the very countries that signed it. Technology has created both new possibilities and new challenges, and it is increasingly likely that states will consider updating existing rules. Additionally, although FTAs are considered a plausible alternative for countries to pick and choose among countries they trust, they are not enough to meet current market needs.

Recommendations:

a. As countries are typically reluctant to cede parts of their sovereignty, international treaties frequently lack clarity and comprehensiveness in order to secure broad approval. Despite this, by interpreting and implementing the general GATS principles, WTO panels have proven a fair amount of effectiveness. Therefore, it is necessary to reinvigorate and consistently utilize these panels to handle new trade and data governance concerns.

b. While it may be challenging to come up with a universal definition of "national security," it is essential to outline certain boundaries or criteria. Doing so would help prevent the abuse of national security exceptions and provide a more stable legal framework for trade and data flow.

c. The GATS framework urgently needs to be modernized to address new technological challenges – particularly those pertaining to online services, cross-border data transfer, and digital transactions. Including explicit provisions on data localization would improve legal certainty and encourage fair competition in the digital economy.

References

[1] Abe, Y. (2021). Data localization measures and international economic law: How do WTO and TPP/CPTPP disciplines apply to these measures? *Public Policy Review, 16*(5), 1–29. https://www.mof.go.jp/english/pri/publication/pp_review/ppr16_05_02.pdf

[2] Bahri, A. (2020). Challenging localization: Analyzing data localization against GATS. *International Journal of Legal Science and Innovation, 2*(3), 337–346. https://www.ijlsi.com/wp-content/uploads/Challenging-Localization-Analyzing-Data-Locali zation-against-GATS.pdf

[3] Bowman, C. (2017, January 6). Data localization laws: An emerging global trend. *JURIST – Hotline*. http://jurist.org/hotline/2017/01/data-localization-laws-an-emerging-global-trend.php

[4] Chander, A. & Le, U. (2014). Breaking the web: Data localization vs the global internet. *UC Davis Legal Studies Research Paper*, No. 378. https://ssrn.com/abstract=2407858

[5] Charter of Fundamental Rights of the European Union (CFR).

[6] Cory, N. (2017, May 1). Cross border data flows: Where are the barriers and what do they cost? *ITIF*. https://itif.org/publications/2017/05/01/crossborder-data-flows-where-are-barriers-and-what-do-they-cost

[7] Cybersecurity Law of the People's Republic of China (2016) (CSL).

[8] Data Security Law of the People's Republic of China (2021) (DSL).

[9] Del Giovane, C., Ferencz, J. & López González, J. (2023). The nature, evolution and potential implications of data localisation measures. *OECD Trade Policy Papers*, No. 278. OECD Publishing. https://doi.org/10.1787/179f718a-en

[10] Devane, H. (2022, January 27). Data localization: A complete overview. *Immuta*. https://www.immuta.com/blog/data-localization/

[11] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 (Data Protection Directive).

[12] European Commission. (2021, June 4). *Updated standard contractual clauses for data transfers*. European Commission. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

[13] Executive Order No. 14117: Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern (2024) (EO 14117).

[14] Fahey, E. (2023). Does the EU's digital sovereignty promote localisation in its model digital trade clauses? *European Papers, 8*(2), 503–511. https://www.europeanpapers.eu/europeanforum/does-eu-digital-sovereignty-promote-localisation

[15] Fraser, E. (2016). Data localisation and the Balkanisation of the internet. *SCRIPTed, 13*(3), 359. https://doi.org/10.2966/scrip.130316.359

[16] Hodson, S. (2019). Applying WTO and FTA disciplines to data localization measures. *World Trade Review, 18*(4), 579–607. https://doi.org/10.1017/S1474745618000277

[17] Inside Privacy. (2022, May 3). Leaked draft version of the European Health Data Space regulation. *Inside Privacy*. https://www.insideprivacy.com/international/european-union/leaked-draft-version-of-the-european-health-data-space-regulation/

[18] Internal Revenue Service. (2021). Publication 1075: *Tax information security guidelines for federal, state, and local agencies* (Rev. 11-2021). https://www.irs.gov/pub/irs-pdf/p1075.pdf

[19] Kyger, L. (2024, August 8). Data localization and other barriers to digital trade. *Hinrich Foundation*. https://www.hinrichfoundation.com/research/article/tech-digital-trade/data-localization

[20] Lu, W. (2024). Data localization: From China and beyond. *Indiana Journal of Global Legal Studies, 31*(1), 183–202. https://muse.jhu.edu/pub/3/article/924201

[21] National Board of Trade. (2014). *No transfer, no trade: The importance of cross-border data transfers for companies based in Sweden*. National Board of Trade. https://unctad.org/system/files/non-official-document/dtl_ict4d2016c01_Kommerskollegium_en.pdf

[22] OECD. (2020). *Data localisation trends and challenges: Considerations for the review of the OECD Privacy Guidelines* (OECD Digital Economy Papers No. 301). OECD. https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/12/data-localisation-trends-and-challenges_d775fe8a/7fbaed62-en.pdf

[23] Outbound Data Transfer Security Assessment Measures (2022) (ODTSAM).

[24] Personal Information Protection Law of the People's Republic of China (2021) (PIPL).

[25] Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons (2024).

[26] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation) (GDPR).

[27] Regulation (EU) 2022/868 of the European Parliament and of the Council (Data Governance Act) (DGA).

[28] Regulation (EU) 2023/2854 of the European Parliament and of the Council (Data Act) (DA).

[29] Regulation on Network Data Security Management (China, 2024) (NDSM Regulation).

[30] Regulations on the Security Protection of Critical Information Infrastructure (China, 2021) (CII Regulations)

[31] Satori Cyber. (2024, December 1). Data localization 101: The essentials. *Satori Cyber*. https://satoricyber.com/cloud-data-governance/data-localization-101-the-essentials/

[32] Singh, J. (2022). Data localization. *Jus Corpus Law Journal, 3*(2), 495–503. https://www.juscorpus.com/wp-content/uploads/2023/01/96.-Jigyasa-Singh.pdf

[33] Tang, A. (2021, July 6). Cross-border data transfer and data localization requirements in China. *ISACA*. https://www.isaca.org/resources/news-and-trends/industry-news/2021/cross-border-data-transfer-and-data-localization-requirements-in-china

[34] Tseng, E. (2024). Data localization: The compatibility with GATS and its outlook. *Michigan Journal of International Law Blog*. https://www.mjilonline.org/data-localization-the-compatibility-with-gats-and-its-outlook/

[35] Whorra, G. (2022). Data localization: An issue beyond borders. *RGNUL Financial and Mercantile Law Review, 9*, 43. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/rlfladme2022&section=7

[36] World Trade Organization. *Argentina – Measures relating to trade in goods and services*. Panel Report of 2015. No. WT/DS453/R.

[37] World Trade Organization. *Argentina – Measures relating to trade in goods and services*. Appellate Body Report of 2016. No. WT/DS453/AB/R.

[38] World Trade Organization. *Korea – Measures affecting imports of fresh, chilled and frozen beef*. Appellate Body Report of 2000. Nos. WT/DS161/AB/R and WT/DS169/AB/R.

[39] World Trade Organization. *Russia – Measures concerning traffic in transit*. Panel Report of 2019. No. WT/DS512/R.

[40] World Trade Organization. *United States – Measures affecting the cross-border supply of gambling and betting services*. Panel Report of 2004. No. WT/DS285/R.

[41] World Trade Organization. *United States – Measures affecting the cross-border supply of gambling and betting services*. Appellate Body Report of 2005. No. WT/DS285/AB/R.

[42] Yakovleva, S. (2018). Should fundamental rights to privacy and data protection be a part of the EU's international trade "deals"? *World Trade Review, 17*(3), 477–508. https://doi.org/10.1017/S1474745617000453

[43] Yakovleva, S. (2024). Personal data transfers in international trade and EU law: A tale of two 'necessities'. In *Governing cross-border data flows: Reconciling EU data protection and international trade law*. Oxford University Press. https://doi.org/10.1093/oso/9780192899248.003.0002