Proceedings of ICILLP 2025 Symposium: Property Law and Blockchain Applications in International Law and Legal Policy
DOI: 10.54254/2753-7048/2025.LD28364

Data Localization and the GATS Public Order Exception: A Legal Examination of China's Cybersecurity Law and the Apple iCloud Guizhou Case

Yunuo Wu

The High School Attached to Northeast University, Changchun, China
18043570669@163.com

Abstract. The rapid growth of cross-border data services has raised concerns about privacy and national security. Taking Article 37 of China's Cybersecurity Law—which underpins Apple iCloud's operational requirements in Guizhou—as a case study, this paper examines whether the policy violates Articles VI (Domestic Regulation), XVII (National Treatment), and XIV(a) (Public Order Exception) of the World Trade Organization's General Agreement on Trade in Services (GATS). Moving from general legal analysis to specific exception application, this study employs textual and case analysis to reveal that this requirement may place foreign service providers at a competitive disadvantage, violating national treatment obligations. Furthermore, it struggles to meet the necessity and minimal restriction criteria for the "public procedure exception." Based on these findings, the paper proposes introducing risk-tiered procedures in data management, adopting alternative solutions that balance localization and security, and enhancing the certainty of WTO rules to achieve equilibrium between data sovereignty and the freedom of trade in services.

Keywords: data localization, national treatment, cybersecurity law, GATS Article XIV, domestic regulation

1. Introduction

In 2017, China enacted the Cybersecurity Law, which requires operators of critical information infrastructure to store personal information and important data within China. A representative case of this policy's tension with national data security is —Apple's relocation of its China iCloud data to Guizhou, an incident that directly impacted the operational models and costs of multinational corporations. This has also sparked related academic research. However, few studies have combined Article 6 (National Regulation), Article 17 (National Treatment), and Article 14 (Exception for Public Order) of the GATS with China's Cybersecurity Law and the Apple case, leaving a research gap. This paper aims to fill this gap through literature review and legal analysis. The objective is not only to analyze China's data localization policy within a comprehensive GATS framework from an academic perspective but also to offer policymakers insights on balancing national security with digital trade obligations.

DOI: 10.54254/2753-7048/2025.LD28364

2. Analysis of national treatment under GATS Article XVII and data localization measures

2.1. Core rules and case law standards for national treatment under GATS Article XVII

GATS Article XVII requires that in a service sector where a member has made commitments, foreign services and service suppliers must be treated no less favorably than domestic ones. This ensures that foreign suppliers enjoy equal competitive conditions. The key is whether the measure alters competitive conditions and disadvantages foreign suppliers. WTO jurisprudence confirms that measures placing foreign suppliers at a disadvantage violate this standard, regardless of their form or purpose [1]. For example, in the EC v. United States et al. (Bananas) dispute, the EC's discriminatory quota and licensing systems for banana imports and distribution were ruled to violate GATS Articles II and XVII because they disadvantaged foreign suppliers [2-4]. The Appellate Body emphasized that the key consideration is whether competitive conditions have been adversely altered, not the intent or form of the measure [2-4].

2.2. China's data localization requirements and impact

Article 37 of China's Cybersecurity Law mandates that operators of critical information infrastructure (CIIOs) store personal information and important data collected or generated within China domestically. Any cross-border transfer requires prior security assessment approval [5]. This requirement, while applicable to all enterprises, disproportionately affects foreign suppliers, who face additional burdens such as investing in local data centers, adjusting encryption and storage systems, and undergoing complex security reviews. Domestic enterprises, however, typically meet these requirements without extra burdens. This increases foreign suppliers' costs and compliance pressures, weakening their competitive position [6-8]. The Apple iCloud case is a prime example, where Apple was compelled to partner with a Guizhou provincial enterprise to establish a data center in Guizhou, storing all Chinese users' iCloud data and encryption keys domestically [9-10].

2.3. Compliance analysis under GATS Article XVII

Under Article XVII, assessing data localization measures hinges on determining whether they deprive foreign service providers of equal competitive conditions with domestic counterparts]. Although Article 37 of China's Cybersecurity Law does not explicitly distinguish based on nationality, its practical effect imposes structural disadvantages on foreign suppliers, such as mandatory localization of infrastructure, higher compliance costs, and complex outbound data transfer assessments [2,5]. This distortion of the competitive environment suggests a breach of the national treatment obligation. If the measure substantially obstructs cross-border data flows, it may simultaneously constitute a market access restriction prohibited under Article XVI.

Even if such breaches are established, China may invoke exceptions like Article XIV for defense. However, it would need to prove that the measures are appropriate, necessary, and not more trade-restrictive than required to meet its security goals [11-12]. Balancing these requirements and justifying the measures under international trade law is a significant challenge.

DOI: 10.54254/2753-7048/2025.LD28364

3. Conflict analysis between GATS Article VI domestic regulation obligations and data localization measures

3.1. Legal framework and academic interpretations

GATS Article VI sets norms for domestic regulation in services trade, emphasizing rationality, transparency, and necessity. Article VI:4 allows the WTO Council to create disciplines for regulatory measures like licensing and technical standards, ensuring they are based on objective criteria and do not form unnecessary trade barriers. Article VI:5 temporarily restricts opaque or discriminatory requirements. Essentially, Article VI balances regulatory autonomy with trade liberalization commitments.

Academic consensus holds that Article VI embodies the WTO's intent to promote "good regulation," introducing necessity and proportionality considerations into non-discriminatory measures. For instance, Tuthill posits that Article VI constitutes the core regulatory rule within the GATS framework, preventing members from using technical regulations as a disguised form of protectionism. Scholars like Bryan Mercurio also note that amid the rise of digital trade, these provisions of Article VI possess "untapped potential" for reviewing whether novel measures—such as data localization requirements—exceed necessary scope and impose undue barriers to trade in services. Mira Burri's research further underscores this point: transparency obligations (GATS Article III) and domestic regulatory obligations (Article VI) offer potential solutions for digital trade issues, yet few disputes have directly invoked them thus far. Statistics indicate that by 2023, over 40 countries globally had implemented approximately 100 data localization measures. Most of these not only mandate local storage but also restrict data outbound transfers, creating new barriers to digital services trade. Article VI of GATS provides a framework for balancing members' autonomy in pursuing legitimate policy objectives against their commitments to liberalize trade in services [4, 13].

3.2. Ambiguity and enforcement challenges in China's regulatory practices

China's data localization regulations, grounded in laws like the Cybersecurity Law, face issues of unclear terminology and broad enforcement discretion. For instance, Article 37 mandates that critical information infrastructure must store personal information and important data collected in China domestically, but relevant terms like "important data" lack clear definitions. This ambiguity was highlighted in 2018 when Apple was compelled to migrate mainland Chinese users' iCloud data to local data centers, raising concerns about user privacy and corporate control over data. Most foreign tech companies unable or unwilling to comply with localization policies have been forced to exit the Chinese market—mandatory data storage and stringent content censorship have significantly constrained the operational space for foreign service providers. The elastic definition of "personal information and important data" grants regulators broad discretionary power, potentially leading to selective enforcement while increasing compliance uncertainty for foreign enterprises. Meanwhile, although China has established a data outbound security review system, it has yet to develop independent judicial remedy channels. Under GATS Article VI:2, members should establish impartial administrative or judicial review mechanisms to provide appeal opportunities for unfavorable decisions affecting service providers. However, China's current data outbound licensing is primarily determined through self-review by administrative bodies, leaving enterprises without effective avenues to appeal review outcomes. This situation remains deficient in procedural transparency and remedial safeguards. Such legal ambiguity, broad enforcement flexibility, and lack

DOI: 10.54254/2753-7048/2025.LD28364

of transparent remedies render China's data localization policies vulnerable to challenges under the WTO framework for failing to meet the requirements of "objective and impartial" administration [4, 9, 10].

3.3. Legal risks of data localization measures violating Article VI

China's Apple iCloud data localization requirement may violate GATS Article VI on two counts. First, objective transparency of procedures and standards. Under GATS Article VI:1, China ensure that all generally applicable measures in its committed service sectors are implemented in a reasonable, objective and impartial manner. However, key concepts like "important data" in China's current regulations remain ambiguous, making regulatory requirements unpredictable for businesses. The enforcement process lacks independent oversight, potentially failing to meet the objective transparency standard. Second, necessity and proportionality of measures. Under Articles VI:4–5, technical requirements should not exceed what is necessary to achieve objectives such as service quality. Mandating all user data storage within China constitutes a stringent technical standard. If such measures lack evidence of necessity and alternatives, they may be deemed "unnecessary trade restrictions," violating Article VI [4, 9, 10]. For example, achieving law enforcement access through cross-border data agreements could be a less restrictive alternative.

Furthermore, even if China asserts its measures aim to protect national security or public morality, they must still satisfy necessity tests and balancing assessments. Article XIV requires measures to be "necessary" to achieve their objectives and implemented through the least trade-restrictive means. The breadth and vagueness of China's data localization policies may make it difficult to pass this test. If sensitive data categories are not differentiated and local storage is uniformly mandated, arbitration bodies may suspect the measures of masking trade restrictions. In summary, Apple's iCloud localization policy carries legal risks of violating GATS Article VI: it could be deemed lacking in objective transparency in administrative enforcement or challenged for disproportionately restricting trade in services. Should China fail to provide sufficient justification for the measure's rationality or undertake necessary adjustments and clarifications, it would face an unfavorable position in potential future trade disputes [4, 9, 10].

In summary, China's Apple iCloud data localization policy reveals systemic design flaws and implementation risks under the GATS framework.This highlights the need for clear legislation and the burden of proof on WTO members to demonstrate the reasonableness of their measures.

4. Legitimacy argument for data localization under the public order exception of GATS Article XIV

GATS Article XIV(a) permits members to adopt exceptional measures on grounds of "public order." However, the WTO Appellate Body has consistently emphasized that such exceptions must satisfy three conditions. As illustrated in the US–Gambling (2005) case, the Appellate Body requires a "necessity" test as the first condition; second, the objective of the measure is legitimate and the measure makes a "substantial contribution" to achieving that objective; third, it must be assessed whether less trade-restrictive alternatives are available [12]. Scholars have also debated the exception clause. Mitchell and Mishra argue its substantive purpose is to prevent members from using security or public order as pretexts for de facto protectionist measures [14]. Similarly Mercurio notes that If a country's measure structurally increases compliance burdens only for foreign service suppliers, it will fail the WTO proportionality test, even if formally applicable to all suppliers. In China, Apple was required to establish a joint venture with Guizhou Cloud Big Data

DOI: 10.54254/2753-7048/2025.LD28364

Industry Group, a state-owned enterprise. All mainland user data is managed by this company, and encryption keys must be surrendered. Apple itself admitted having “no choice,” stating in interviews that compliance was entirely a forced outcome. This arrangement raises two major issues under WTO scrutiny:

First, there is a clear issue of discrimination. Domestic firms like Alibaba Cloud are not required to form joint ventures with state-owned enterprises or surrender encryption keys. Second, the policy is excessively broad. It mandates data localization for all types of data without distinguishing between different data categories based on their varying risk levels. Similar concerns have been raised by scholars such as Mira Burri, who has noted that China's iCloud model lacks necessity and proportionality. According to Burri, there is no direct causal link demonstrated between comprehensive localization and national security [9-10].

In contrast, Russia's Personal Data Law, which has been in effective since 2015, mandates foreign companies to store personal data of Russian citizens locally. This is similarly justified on grounds of “national security” and “sovereignty.” LinkedIn was banned for non-compliance, while Facebook and Twitter faced fines. Scholar Hernández-Ramos notes that Russia's approach “almost inevitably raises national treatment issues under WTO frameworks” due to its significant increase in compliance costs for foreign firms [15-16]. Unlike China, however, Russia does not compel foreign companies to hand over encryption keys or partner with state-owned enterprises. Companies retain some autonomy in choosing compliance methods. This indicates that while Russia's measures exhibit discriminatory tendencies, their level of intervention is less extensive than China's. This article argues that if Russia's localization constitutes a market access barrier, China's iCloud model represents comprehensive intervention in corporate operational structures. This makes China's measures more susceptible to being deemed excessive under WTO scrutiny.

Integrating the perspectives of the scholars, several conclusions emerge: First, national security justifications may hold merit, but invoking exceptions requires demonstrating a direct link to comprehensive localization. Second, classified data constitutes only a portion of total information. China has not proven all data involves national security concerns, while alternative solutions exist, such as independent key escrow, encryption audits and secure multi-party computation. Therefore, this paper contends that China's iCloud case would likely be found to fail to meet the “necessity and proportionality” requirements of Article XIV(a) of the GATS.

5. Recommendations

First, to address the ambiguity raised regarding Domestic Regulation (Art. VI), China should further define the scope of important data in legislation and implementing rules to enhance transparency. Adopting a risk-based approach, it should cover only data genuinely involving national security or public interest. A unified industry catalog and determination criteria should be established to reduce discretionary enforcement and ensure foreign enterprises can anticipate regulatory requirements.

Second, to address the remedial deficiencies in Domestic Regulation, an independent review or appeal mechanism should be created to ensure foreign enterprises receive impartial review when facing adverse decisions. This would not only enhance the legitimacy and credibility of China's regulatory framework but also mitigate the risk of being deemed “lacking objectivity” in WTO disputes. Scholars (e.g., Mercurio, Burri) emphasize that transparency and redress are critical conditions for ensuring regulations comply with Article VI [6].

Given the current lack of detailed WTO rules on data flows, China and other members should urge the Dispute Settlement Body or the Council for Trade in Services to issue an “interpretative declaration” clarifying the following points: under what circumstances data localization may

DOI: 10.54254/2753-7048/2025.LD28364

constitute a legitimate exception under Article XIV; how to apply the "necessity and proportionality test"; and how the burden of proof should be allocated among members. These measures would reduce future legal uncertainties and enhance the international acceptability of China's measures.

6. Conclusion

The Apple iCloud data localization case in China demonstrates that China's security-based data localization requirements may pose potential legal risks under the WTO framework. Such measures may be deemed to unnecessarily restrict trade in services (violating GATS Article VI) and impose additional costs on foreign service providers (breaching GATS Article XVII national treatment), thereby constituting excessive trade restrictions and discrimination. Even if China intends to invoke the "public order" exception under Article XIV(a) of GATS to justify this, WTO precedent indicates an extremely low success rate for such national security measures passing strict necessity tests. In practice, out of 44 invocations of general exceptions, only one has succeeded. Therefore, while safeguarding cyber sovereignty and national security, China should ensure relevant measures are transparent, non-discriminatory, and restricted to the extent necessary to minimize the likelihood of being deemed discriminatory or an unnecessary restriction on trade.

However, this study primarily relies on textual analysis and case commentary, lacking empirical data on corporate compliance costs and trade impacts. Future research should incorporate quantitative methodologies, such as surveys, econometric analyses, and cost-benefit assessments, to provide a more robust and evidence-based evaluation.

References

[1] World Trade Organization. (1995). General Agreement on Trade in Services (GATS) — Text. https: //www.wto.org/english/docs_e/legal_e/26-gats.pdf
[2] World Trade Organization. (1995). WTO Analytical Index, GATS — Article XVII (Jurisprudence): National Treatment. https: //www.wto.org/english/res_e/publications_e/ai17_e/gats_art17_jur.pdf
[3] World Trade Organization. (1997). Appellate Body Report, European Communities — Regime for the Importation, Sale and Distribution of Bananas (EC — Bananas III), WT/DS27/AB/R. https: //www.wto.org/english/tratop_e/dispu_e/27abr.pdf
[4] World Trade Organization. (1995). WTO Analytical Index, GATS — Article VI (Practice): Domestic Regulation. https: //www.wto.org/english/res_e/publications_e/ai17_e/gats_art6_oth.pdf
[5] Creemers, R., Webster, G., & Triolo, P. (2018). Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017). https: //digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/
[6] Organisation for Economic Co-operation and Development. (2019). Trade Policy Paper No. 278: The nature, evolution and potential implications of data localisation measures. https: //www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2019)19/FINAL&docLanguage=En
[7] Chander, A., & Le, U. P. (2014). Breaking the Web: Data Localization vs. the Global Internet. Emory Law Journal. https: //papers.ssrn.com/sol3/papers.cfm?abstract_id=2407858#paper-references-widget
[8] Kuner, C. (2015). Data Nationalism and Its Discontents. Emory Law Journal Online. https: //scholarlycommons.law.emory.edu/elj/
[9] Apple Inc. (2024). iCloud operated by GCBD — Terms and Conditions. https: //www.apple.com/legal/internet-services/icloud/en/gcbd-terms.html
[10] Nellis, S., & Cadell, C. (2018). Apple moves to store iCloud keys in China, raising human rights fears. Reuters. https: //www.reuters.com/article/technology/apple-moves-to-store-icloud-keys-in-china-raising-human-rights-fears-idUSKCN1G805Z/
[11] World Trade Organization. (1995). WTO Analytical Index, GATS — Article XIV (Jurisprudence): General Exceptions. https: //www.wto.org/english/res_e/publications_e/ai17_e/gats_art14_jur.pdf

DOI: 10.54254/2753-7048/2025.LD28364

[12] World Trade Organization. (2005). Appellate Body Report, United States — Measures Affecting the Cross-Border Supply of Gambling and Betting Services (US — Gambling), WT/DS285/AB/R. https: //www.wto.org/english/tratop_e/dispu_e/cases/ab_reports_e.htm?WT/DS285/AB/R
[13] Organisation for Economic Co-operation and Development. (2019). Trade Policy Paper No. 278: The nature, evolution and potential implications of data localisation measures. https: //www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2019)19/FINAL& docLanguage=En
[14] Mitchell, A. D., & Mishra, N. (2019). Regulating cross-border data flows in a data-driven world: how WTO law can contribute. Journal of International Economic Law, 23(1), 65-97. https: //academic.oup.com/jiel/article-abstract/23/1/65/5627761?redirectedFrom=fulltext
[15] Savelyev, A. (2016). Russia's new personal data localization regulations: A step forward or a self-imposed sanction? Computer Law & Security Review, 32(3), 426-440. https: //www.sciencedirect.com/science/article/abs/pii/S0267364915001703?via%3Dihub
[16] Morgan Lewis. (2021). Data Localization Laws: Russian Federation (Q& A overview). https: //www.morganlewis.com/-/media/files/publication/outside-publication/article/2021/data-localization-laws-russian-federation.pdf