Advances in Social Behavior Research Vol.16 Issue 10 EWA Publishing
Available Online: 17 November 2025 DOI: 10.54254/2753-7102/2025.29816

Conflicts and coordination paths in the trade regulation of data localization measures—from the perspective of GATS and regional trade agreements

Qumeng Ye

Macau University of Science and Technology, Macau, China

3250006504@student.must.edu.mo

Abstract. Against the backdrop of the rapid expansion of the digital economy, cross-border data flows have become the core foundation for the development of digital trade. As a key institutional instrument for countries to balance data security and privacy protection, data localization measures increasingly conflict with international trade rules. These conflicts not only hinder the smooth progress of global digital trade but have also emerged as a central issue in global digital governance, attracting broad attention from governments, international organizations, and academia. Taking the legal nature of data localization measures as its logical starting point, this paper conducts a systematic analysis of the regulatory conflicts between such measures and digital trade within the framework of the General Agreement on Trade in Services (GATS) and regional trade agreements such as the Trans-Pacific Partnership (TPP), the United States–Mexico–Canada Agreement (USMCA), and the Regional Comprehensive Economic Partnership (RCEP). It explores the specific manifestations and impacts of these conflicts under different trade scenarios, while also mapping the diverse characteristics of data governance models across countries and regions. Through a comparative study of the data governance philosophies, legal systems, and policy practices of major economies—including the United States, the European Union, and China—the paper proposes a coordination path for resolving such conflicts based on the principle of technological neutrality and the "principle-plus-exception" framework. The findings of this study not only enrich the theoretical system of global digital trade governance but also provide important theoretical and practical references for China's active participation in the formulation of international digital trade rules, the enhancement of its discourse power in global digital governance, and the promotion of the healthy and orderly development of its digital trade.

Keywords: data localization, digital trade, GATS, regional trade agreements, cross-border data flow

1. Introduction

1.1. Research background

The rapid iteration of information technology and the widespread adoption of the Internet have propelled human society into the era of the digital economy. As the key productive factor of this new era, data holds strategic value comparable to that of "digital oil." Cross-border data flows, as the core link in digital trade, directly determine its scale, efficiency, and quality. From a global perspective, digital trade now encompasses a wide range of sectors including e-commerce, digital services, and cross-border data transmission. In 2023, the total value of global digital trade exceeded USD 30 trillion, making it a new engine for global economic growth.

However, while cross-border data flows have unleashed trade dividends, they have also brought mounting risks to data security and privacy protection. In 2024, over 100,000 global data breach incidents were recorded, involving the leakage of more than 5 billion items of personal information. Practices such as overseas surveillance and data misuse not only threaten citizens' legitimate rights and interests but may also endanger national security and public order. In response, many countries have introduced data localization measures to ensure data security by restricting the geographical scope of data storage, processing, and transmission.

Article 37 of China's Cybersecurity Law explicitly stipulates that operators of critical information infrastructure must store within the territory of China any personal information and important data collected domestically, and that data transfers abroad are subject to a mandatory security assessment [1]. By imposing territorial restrictions, this provision seeks to mitigate the risks

of outbound data transfer and safeguard national cybersecurity and citizens' informational rights. Similarly, Australia's Personally Controlled Electronic Health Records Act (PCEHR) establishes strict requirements for the offshore processing of medical data, allowing only de-identified medical records to be transferred abroad after approval, thereby protecting citizens' medical privacy and preventing cross-border data leakage [2].

Although such measures pursue legitimate policy objectives, they generate significant tension with the principles of trade liberalization embodied in the General Agreement on Trade in Services (GATS). GATS promotes the free flow of services across borders, whereas data localization, by imposing territorial restrictions, hampers the cross-border provision of digital services, thereby conflicting with the spirit of the Agreement [3]. Furthermore, regional trade agreements such as the Trans-Pacific Partnership (TPP), the United States–Mexico–Canada Agreement (USMCA), and the Regional Comprehensive Economic Partnership (RCEP) diverge considerably in their approaches to data localization—the TPP and USMCA adopt a restrictive stance, while the RCEP maintains a more flexible and inclusive attitude. This fragmentation of rules has exacerbated uncertainty in international digital trade, exposing enterprises to increasingly complex compliance environments and significantly raising both operational costs and regulatory risks [4,5].

1.2. Research significance

1.2.1. Theoretical significance

Existing studies largely focus on the domestic legal compliance of data localization measures, while insufficient attention has been paid to their conflicts and possible coordination with international trade rules. This paper begins by defining the legal nature of data localization measures and, through an analysis of the relevant provisions in GATS and regional trade agreements, systematically explores the manifestations and underlying causes of regulatory conflicts. It then examines the differences in national data governance models and proposes a coordination framework based on the principles of technological neutrality and "principle plus exception." This study thus bridges the research gap between international trade rules and domestic regulatory practices.

Moreover, the coordination path proposed in this paper provides a new theoretical perspective for global digital trade governance. It breaks away from the binary thinking of "either complete free flow or strict localization," and advances theoretical innovation toward a balanced model of security and freedom, thereby offering a conceptual foundation and reference for future studies in this field.

1.2.2. Practical significance

At the practical level, this research offers valuable insights for China's participation in the formulation of international digital trade rules. Although China's digital trade has maintained an average annual growth rate of 15%, its influence in international rule-making remains limited, facing increasing regulatory pressure from developed economies. By analyzing the evolution of international rules and the divergence among regional agreements, this paper proposes a coordination strategy aligned with China's national interests, which can serve as a policy reference for government agencies during international negotiations, helping to safeguard national data security and trade interests.

In addition, the findings can provide compliance guidance for enterprises. By clarifying the focal points of conflict and the direction of coordination between data localization measures and international trade rules, the study helps enterprises better understand regulatory differences across jurisdictions, reduce compliance costs and operational risks in cross-border activities, and enhance the global competitiveness of Chinese digital enterprises—thereby facilitating the implementation of China's "going global" digital strategy.

1.3. Current research status

1.3.1. Domestic research status

Domestic research on data localization primarily focuses on three aspects. First, the legitimacy of data localization measures: scholars generally affirm their necessity from the perspectives of national security and privacy protection, while also acknowledging potential downsides such as increased corporate costs and impediments to trade. Second, the construction of domestic legal systems: studies based on the Cybersecurity Law and the Data Security Law explore ways to improve existing frameworks and propose concrete measures such as classified and graded management as well as mandatory security assessments. Third, the compliance practices of enterprises: this line of research emphasizes practical procedures for data storage and outbound data approval, providing enterprises with risk prevention strategies.

Nevertheless, existing domestic studies reveal clear limitations. Most of them remain confined to the national legal level, offering insufficiently in-depth analysis of the rules under GATS and regional trade agreements. As a result, they fail to systematically identify the key points of conflict between data localization and international trade norms, nor do they propose comprehensive coordination strategies from a global perspective.

1.3.2. Foreign research status

Foreign research on data localization emerged earlier and shows a clear divergence in perspectives. Some scholars, adopting a trade liberalization viewpoint, criticize data localization as a new form of trade barrier that contravenes GATS principles and call for the removal of such restrictions. Others, acknowledging its necessity for security protection, focus on how to balance data security with the facilitation of trade. Additionally, comparative studies of the data governance models in the United States, the European Union, and Japan have been conducted to provide references for international regulatory coordination [6,7].

However, foreign research also exhibits two major shortcomings. First, many studies focus excessively on a single dimension —either trade freedom or security protection—while lacking a balanced analytical perspective. Second, they pay insufficient attention to the particularities of data localization in developing countries, often overlooking disparities in technological capacity and industrial foundations. Consequently, the proposed coordination approaches tend to have limited applicability in developing-country contexts.

1.4. Research methods and framework

1.4.1. Research methods

1.4.1.1. Literature review

This study reviews domestic and international academic literature, international treaties (such as GATS and TPP), regional trade agreements (such as USMCA and RCEP), and policy documents (including the Cybersecurity Law and the Data Security Law). This enables a comprehensive understanding of the theoretical developments and legal texts related to data localization and international trade regulation, providing a solid theoretical foundation for further analysis.

1.4.1.2. Comparative analysis

Through a comparative examination of national data governance models—such as the U.S. model of "industry self-regulation and liberalism," the EU model of "government regulation and privacy priority," and the Chinese model of "sovereignty priority and classified regulation"—this method analyzes how GATS, TPP, USMCA, and RCEP differ in their regulatory approaches toward data localization, thereby identifying focal points of conflict and drawing lessons for coordination.

1.4.1.3. Case study

Using Article 37 of China's Cybersecurity Law and Australia's PCEHR Act as representative cases, this method explores how conflicts between data localization and trade liberalization manifest in practice and assesses their real-world implications, enhancing the empirical relevance of the study.

1.4.1.4. Normative analysis

Drawing upon theories from law and international trade, this method conducts a normative examination of the legal attributes of data localization and the conflicts within trade rules to ensure that the proposed coordination path aligns with both legal logic and trade principles.

1.4.2. Research framework

This paper is structured into six chapters: Chapter 1: Introduction — outlines the research background, significance, current status, methods, and framework. Chapter 2: The Legal Nature and Typology of Data Localization Measures — defines their dual attributes and classifies various types and features of such measures. Chapter 3: Conflicts Between Data Localization and the Principles of GATS and Regional Trade Agreements — analyzes the nature and mechanisms of these conflicts. Chapter 4: Deep-Seated Causes of the Conflicts — investigates differences in governance models and value priorities among countries. Chapter 5: Paths for Conflict Coordination — proposes strategies based on the principle of technological neutrality, the "principle plus

exception" framework, and regional rule alignment. Chapter 6: Conclusion — summarizes key findings, identifies research limitations, and provides directions for future studies.

2. Legal attributes and typological analysis of data localization measures

2.1. Defining the legal attributes of data localization measures

2.1.1. An expression of national data regulatory sovereignty

In the digital economy era, data has become a strategic national resource, and data sovereignty has emerged as an essential component of state sovereignty. Data localization measures serve as a concrete manifestation of a state's exercise of data regulatory sovereignty. By legislating the territorial scope of data storage and processing, governments can effectively control data resources and safeguard national security and public interests.

Article 2 of China's Data Security Law explicitly states that "data security work shall adhere to the overall national security outlook," thereby incorporating data security into the national security framework. Data localization requirements are the institutional embodiment of this concept—by mandating domestic storage, the state ensures control over critical data and prevents foreign entities from obtaining information that may jeopardize national security. From the international perspective, the principle of sovereign equality established in the Charter of the United Nations provides a legal foundation for national data regulatory authority. Most countries recognize the legitimacy of exercising jurisdiction over data generated within their territories. Accordingly, data localization measures possess a solid basis in international law and sovereign rights.

2.1.2. The dual characteristics of data localization

2.1.2.1. The attribute of "legitimate public policy"

The "legitimate public policy" nature of data localization measures is acknowledged within international trade rules. Article 14 of the Trans-Pacific Partnership (TPP) lists the "protection of consumers, personal information, and cybersecurity" as legitimate policy objectives, affirming the necessity of such measures in safeguarding public interests [4]. In practice, data localization can effectively mitigate risks of data leakage and misuse, thus protecting personal privacy and maintaining public order. For instance, Australia's PCEHR imposes strict limitations on the cross-border transfer of medical data, thereby protecting citizens' medical privacy and preventing rights violations resulting from cross-border data leaks [2]. Similarly, China's domestic storage requirement for credit information ensures financial market stability and prevents financial risks arising from credit data misuse [8]. Furthermore, data localization can stimulate domestic industry development, encourage innovation in data storage and processing technologies, create employment opportunities, and accelerate the transformation of the digital economy—aligning with long-term public interest goals.

2.1.2.2. The attribute of "measures affecting trade in services" under GATS

At the same time, data localization measures fall within the category of "measures affecting trade in services" as regulated under the General Agreement on Trade in Services (GATS). GATS defines four modes of trade in services, with cross-border supply being the primary mode for digital services. Since data constitutes the core production input for digital services, localization requirements that compel service providers to establish data centers domestically restrict data flows across borders, increase operational costs, and hinder the cross-border supply of digital services—thus conflicting with GATS's objective of promoting trade liberalization [3].

For example, if a country mandates that foreign cloud service providers must establish local data centers before offering services, this requirement compels additional capital investment and operational expenses, raising market entry barriers. Such a measure effectively limits cross-border cloud service delivery and contravenes GATS's market access principle.

2.1.3. The tension arising from dual attributes

The dual attributes of data localization measures—reflecting both sovereign regulation and trade liberalization constraints—create an inherent tension. On one hand, states implement localization measures based on sovereign concerns to ensure national security and public welfare; on the other hand, these same measures may contravene key principles of international trade law, such as market access and non-discrimination. Conversely, if states were to fully adhere to trade liberalization principles and abolish localization requirements, they would face heightened data security risks. This tension frequently leads to trade disputes in practice. For instance, a country's requirement that foreign enterprises store financial data domestically has been challenged by

trading partners as a form of "disguised protectionism," allegedly violating GATS's national treatment principle—domestic firms face a simpler data export approval process, while foreign enterprises must undergo multi-agency evaluations [3]. Hence, how to balance the exercise of data regulatory sovereignty with the pursuit of trade liberalization has become a central challenge in the governance of digital trade.

2.2. Typological review of data localization measures

2.2.1. Narrow-scope localization measures

2.2.1.1. Scope of application and typical cases

This type of measure targets only specific categories of sensitive data, prohibiting their storage and processing abroad, with outbound transfers permitted solely under statutory exceptions. The scope mainly covers sectors related to privacy or public interests, such as healthcare, finance, and credit reporting. Typical cases include:

Australia's PCEHR System: It requires that medical records containing personal information be processed domestically, while records without personal information may be transferred abroad only after approval. This framework ensures precise protection of medical privacy and prevents cross-border leakage of sensitive health data [2].

China's Regulations on the Administration of the Credit Reporting Industry: These regulations stipulate that credit reporting agencies must store credit data domestically, and any provision of such data abroad requires prior approval from supervisory authorities. The purpose is to prevent misuse of personal credit information and maintain the stability of the financial credit system [8].

2.2.1.2. Regulatory objectives and trade impacts

Regulatory Objectives: The core objective is to protect sensitive data security and personal privacy while maintaining order in specific industries. By precisely restricting the flow of sensitive data, these measures safeguard security with minimal interference in overall trade activities.

Trade Impacts: The overall impact on digital trade is limited, as only industries involving sensitive data are slightly affected. Although enterprises must bear compliance costs to meet localization requirements, the narrow scope renders these costs manageable. However, differences among countries in defining "sensitive data" may increase compliance risks for cross-border operations.

2.2.2. Broad-scope localization measures

2.2.2.1. Scope of application and typical cases

These measures require all data—regardless of whether it contains personal information—to be stored and processed domestically, allowing cross-border transfers only under exceptional circumstances. The scope covers multiple sectors, including finance, public administration, and big data. Typical cases include:

Russia's Financial Data Localization: All transaction data and client information held by domestic financial institutions must be stored within the country, with outbound transfer prohibited. This comprehensive control framework aims to safeguard financial security and prevent foreign interference in domestic financial markets.

India's Government Data Localization: All administrative data collected by government departments—including policy documents and citizens' identity information—must be stored domestically and may not be transferred abroad. The objective is to protect national political security and administrative order.

2.2.2.2. Regulatory objectives and trade impacts

Regulatory Objectives: The primary aim is to maximize national data security and information sovereignty, comprehensively preventing risks arising from cross-border data flows. At the same time, such measures seek to nurture domestic data industries by leveraging data concentration to drive technological innovation and industrial development.

Trade Impacts: The impact on digital trade is substantial. Increased operational costs: Enterprises are compelled to build large-scale domestic data centers and invest heavily in hardware and human resources. Obstruction of global digital value chain integration: Restricted data flows hinder multinational enterprises from optimizing global resource allocation. Potential trade disputes: Other countries may perceive such measures as trade barriers and resort to the WTO dispute settlement mechanism [3].

3. Conflicts between data localization measures and international trade rules

3.1. Conflicts with the basic principles of GATS

3.1.1. Overview of the basic principles of GATS

The General Agreement on Trade in Services (GATS) establishes four core principles that form the foundation of global trade in services:

(1) Most-Favored-Nation (MFN) Treatment Principle: Members are required to accord services and service suppliers of any other Member treatment no less favorable than that accorded to like services and service suppliers of any other country, thereby eliminating discriminatory arrangements among Members [3].

(2) National Treatment Principle: In sectors where specific commitments have been undertaken, Members must accord foreign service providers treatment no less favorable than that given to domestic providers, ensuring fair competition for foreign suppliers [3].

(3) Market Access Principle: Members must specify the conditions of market access in their Schedules of Commitments and are prohibited from imposing limitations on the number of suppliers, the volume of transactions, or the geographical scope of operations unless such restrictions are explicitly listed as exceptions [3].

(4) Transparency Principle: Members must promptly publish laws, regulations, policies, and administrative procedures related to trade in services to ensure predictability and transparency [3].

3.1.2. Conflicts with the market access principle

3.1.2.1. Core requirements of the market access principle

Under the GATS, Members are required to specify in their Schedules of Commitments the service sectors they have agreed to open and the corresponding access conditions. They may not impose restrictions beyond their commitments, particularly those that "limit the geographic scope of suppliers" or "restrict modes of supply." The core objective is to eliminate market access barriers and facilitate the free flow of services [3]. In the digital services sector, the market access principle prohibits Members from imposing unreasonable restrictions on cross-border delivery of digital services, ensuring that foreign service suppliers may enter the market under the terms of their commitments.

3.1.2.2. Manifestations of conflict

Restricting the Geographical Scope of Service Providers: Data localization measures often require foreign service providers to establish data centers within the territory of the regulating Member, which essentially restricts their geographical scope of operation. If such a measure is not listed as an exception in the Member's Schedule of Commitments, it constitutes a violation of GATS obligations [3]. For example, if a country commits to allowing cross-border delivery of cloud computing services but later mandates that foreign cloud providers must establish domestic data centers, such a requirement effectively prevents cross-border delivery and compels providers to enter the market through "commercial presence," thereby breaching its market access commitments.

Raising Market Entry Thresholds: Data localization measures significantly increase the cost of market entry, imposing disproportionate burdens on small and medium-sized enterprises (SMEs). For instance, if a small country requires foreign big-data analytics firms to build domestic data centers, the necessary investment—often amounting to several million U.S. dollars—far exceeds what SMEs can afford. This results in market exclusion and restricted competition, running counter to the GATS objective of expanding market openness [3].

Restricting the Choice of Supply Modes: GATS permits service providers to freely choose among four modes of supply. Data localization, however, constrains the use of cross-border delivery (Mode 1) [3]. For example, online education and cloud computing services are best delivered via cross-border supply. Yet, due to localization requirements, providers are forced to adopt the "commercial presence" mode, increasing operational costs and reducing service efficiency—thus violating the principle of freedom to choose supply modes.

3.1.3. Conflicts with the non-discrimination principle

3.1.3.1. Core requirements of the non-discrimination principle

The non-discrimination principle comprises the Most-Favored-Nation (MFN) treatment and National Treatment principles. The former ensures equal treatment for all Members' service suppliers, while the latter guarantees fair competition between domestic and foreign providers. The essence of this principle lies in eliminating discriminatory treatment based on nationality or origin [3].

3.1.3.2. Manifestations of conflict

Violation of the National Treatment Principle: Some countries impose more stringent approval procedures on foreign service providers. For instance, a country may require foreign enterprises seeking to transfer data abroad to undergo a joint assessment by the Cyberspace Administration, Ministry of Industry and Information Technology, and Customs, with a review period of up to three months; whereas domestic enterprises need approval only from the Cyberspace Administration, with a one-month review period [3]. Such differential treatment places foreign companies at a disadvantage in cross-border data transfers, violating the National Treatment principle and potentially leading to trade remedy actions. In addition, certain jurisdictions impose stricter compliance requirements on foreign enterprises—such as mandating complex data security management systems and periodic submission of detailed reports—while exempting domestic companies from equivalent obligations, thereby further distorting fair competition [3].

Violation of the Most-Favored-Nation Treatment Principle: Although direct violations of the MFN principle are relatively rare, "differentiated policies" are sometimes observed in practice. For example, a country may sign a bilateral agreement with Country A that simplifies data export approval procedures for its service providers, while maintaining strict scrutiny for providers from other countries. This preferential treatment grants Country A's suppliers a competitive advantage, contravening the MFN requirement of "non-discriminatory treatment" and undermining a fair and level playing field.

3.2. Divergent approaches to data localization in regional trade agreements

3.2.1. The restrictive stance of the TPP and USMCA

3.2.1.1. Regulation of data localization under the TPP

Although the Trans-Pacific Partnership (TPP) recognizes the legitimate public policy objectives underlying data localization—such as protecting security and privacy—it imposes strict limitations on its use.First, it prohibits Members from using data localization as a tool of trade protectionism, requiring that such measures must serve legitimate objectives like security or privacy protection rather than restricting foreign service providers.Second, it adopts the necessity principle, allowing localization only when no less trade-restrictive alternatives are available.

For instance, if a Member State wishes to safeguard personal information, it must first assess whether technical measures such as encryption or security audits can achieve the same objective. Only if such alternatives prove insufficient may the country impose data localization requirements [4]. This approach significantly narrows the scope for localization measures, prioritizing the free flow of data and the liberalization of trade in digital services.

3.2.1.2. Regulation of data localization under the USMCA

The United States–Mexico–Canada Agreement (USMCA) adopts an even stricter position, expressly prohibiting Member States from requiring data to be stored or processed within their territory, except in narrowly defined circumstances—such as for reasons of national security or public order [9]. Moreover, its so-called "poison pill" clause forbids Members from concluding digital trade agreements with non-market economies that grant more favorable treatment than the USMCA does, thereby restricting the regulatory autonomy of its Members [9].

For example, if a USMCA Member State were to sign a digital trade agreement with China granting Chinese enterprises more flexible data localization conditions, such action would violate the poison pill clause and could result in retaliatory measures from other Member States [9]. This clause not only imposes severe restrictions on data localization but also seeks to shape global digital trade governance by excluding non-market economies from participating in rule-making processes.

3.2.2. The Flexible and coordinated approach of the RCEP

3.2.2.1. Characteristics of data localization regulation under the RCEP

The Regional Comprehensive Economic Partnership (RCEP), taking into account the diverse economic and technological capacities of its Members, adopts a flexible and inclusive approach. First, it does not explicitly prohibit data localization measures, allowing Members to adopt such policies on grounds of national security or public order. Second, it emphasizes "cooperation to facilitate cross-border data flows", encouraging Members to reduce trade barriers through consultation and mutual understanding. Third, it upholds the transparency principle, requiring Members to disclose the legal basis, scope, and application of such measures to ensure predictability [5].

This approach respects the regulatory needs of developing economies while leaving room for coordination and gradual rule convergence. It reflects a balance between safeguarding sovereignty and promoting regional digital trade liberalization.

3.2.2.2. Challenges and opportunities of the flexible approach

1. Challenges – Ambiguity and Divergent Interpretations: The lack of clear definitions for "national security" and "public order" in RCEP may lead to divergent interpretations among Members. Some countries could expand the scope of localization by invoking "public interest" to justify hidden trade barriers [5].For instance, a Member State might classify ordinary e-commerce data as being related to "public order" and require it to be stored domestically, thereby increasing compliance costs for enterprises.

2. Opportunities – Policy Space for Developing Economies: RCEP's flexibility provides developing countries with valuable policy space to formulate data localization policies suited to their technological capabilities and industrial foundations, avoiding potential security risks that could arise from overly stringent liberalization. At the same time, the provision on "cooperation to promote data flow" offers a platform for regional coordination. Through consultation, Members can work toward harmonized data classification standards and unified security assessment procedures, thereby reducing regulatory fragmentation and advancing digital trade integration within the region [5].

4. Deep-seated causes of trade-regulatory conflicts over data localization measures

4.1. National differences in data governance models

4.1.1. The United States' "industry self-regulation + liberalism" model

4.1.1.1. Core features of the model

The U.S. model is market-driven with relatively limited government intervention. First, it relies heavily on industry self-regulation: digital firms (e.g., Google, Meta) govern data-handling practices through internal privacy policies and industry codes of conduct, while the Federal Trade Commission (FTC) intervenes mainly through ex post enforcement. Second, it adheres to a liberal philosophy that prioritizes the free flow of data, viewing restrictions on data movement as impediments to innovation and trade.

The emergence of this model is closely linked to the leading position of the U.S. digital economy—U.S. digital firms account for some 70% of the global market, and unrestricted data flows maximize their commercial interests [10]. For example, Google optimizes its search algorithms and ad targeting through global data flows, and Meta relies on cross-border social data to drive user growth; data localization would directly affect their global operational layouts.

4.1.1.2. Impact on international rules

The United States promotes the internationalization of its model through agreements such as the TPP and USMCA: first, by including strict provisions that limit data localization—anchoring rules in the "necessity" principle and prohibitions on localization [4,9]. Second, by employing "poison pill" clauses that restrict Members from entering into more favorable digital trade arrangements with non-market economies, thus constraining Members' rule-making autonomy [9].

While this strategy facilitates the global expansion of U.S. firms, it also exacerbates rule fragmentation—developing countries find overly liberal rules difficult to accept and therefore enact their own localization laws, intensifying conflicts among international rules [5].

4.1.2. The European Union's "government regulation + privacy priority" model

4.1.2.1. Core features of the model

The EU model centers on governmental regulation and places privacy protection at the forefront. First, it establishes a stringent legal framework through the General Data Protection Regulation (GDPR), granting data subjects rights of access, erasure, and rectification, and requiring enterprises to obtain explicit consent for data processing [6]. Second, it allows Member States to adopt localization measures on grounds of public security, thereby balancing privacy protection with national security concerns.

For example, EU Member States may require domestic storage of medical or biometric data to guard against cross-border leaks; at the same time, GDPR's extraterritorial reach obliges non-EU enterprises processing EU citizens' data to comply with EU standards or face substantial fines [6].

4.1.2.2. Impact on international rules

The EU advances its model globally through the extraterritorial effect of the GDPR and international cooperation: over 100 countries have drawn on the GDPR in crafting national data protection laws, promoting convergence toward stronger privacy standards [6]. In international negotiations, the EU pushes to include "privacy protection" within digital trade rules and to require other countries to recognize EU privacy standards, otherwise restricting data flows [6].

This approach enhances the EU's voice in digital governance but may create "regulatory barriers"—developing countries lacking the technical and enforcement capacity to meet EU standards may see cross-border data flows impeded, deepening rule conflicts with the EU [5].

4.1.3. China's "sovereignty first + tiered regulation" model

4.1.3.1. Core features of the model

China's model is grounded in safeguarding data sovereignty and implements classified, tiered management. First, laws such as the Cybersecurity Law and the Data Security Law establish a three-tier protection system of "national security — public interest — personal privacy," clarifying state jurisdiction over data [11]. Second, data are classified and managed by tiers: core data are prohibited from leaving the territory; important data may be transferred abroad only following a security assessment; ordinary data may flow freely [11].

For instance, core data (e.g., military or critical infrastructure data) are strictly confined to domestic storage; important data (e.g., financial transaction or medical data) require security assessment prior to outbound transfer; ordinary data (e.g., enterprise product information) can be transferred across borders, aiming to strike a balance between security and freedom [11].

4.1.3.2. Differences from and conflicts with U.S. and EU models

1. Conflict with the U.S. Model: The U.S. privileges free movement of data and opposes localization [9], while China emphasizes sovereignty and applies localization to core and important data [11]. This ideological divergence produces rule conflicts—for example, the U.S. criticizes China's localization measures as trade barriers, whereas China defends them as necessary for national security, making consensus in international negotiations difficult [3].

2. Conflict with the EU Model: The EU prioritizes privacy and expects global data processing to meet GDPR standards [6], while China seeks to balance security and privacy and adopts distinct privacy enforcement standards [6]. For example, the EU may deem China's enforcement insufficient and refuse adequacy recognition, restricting Sino-EU data flows; China, conversely, views EU standards as overly stringent and ill-suited to developing country realities. These regulatory differences hinder bilateral digital trade and aggravate rule-based conflicts [5].

4.2. The coordination dilemma from the plurality of data values

4.2.1. The economic value and security value of data

4.2.1.1. Manifestations of economic value

The economic value of data is manifested in three main ways. First, it drives growth in digital trade: cross-border data flows underpin digital services such as cloud computing and big-data analytics — in 2023, an estimated 60% of global digital services trade relied on cross-border data flows [10]. Second, data promotes industrial upgrading by optimizing production processes and enabling product and service innovation; for example, industrial data mining has improved manufacturing productivity by about

30% [10]. Third, data-related industries (such as data storage and analytics) generate employment, supporting over 50 million jobs worldwide.

Data localization increases corporate costs. For instance, a multinational corporation might need to invest an additional USD 20 million to build an onshore data center to comply with localization requirements [10], reducing data utilization efficiency and impeding global value-chain integration.

4.2.1.2. Manifestations of security value

The security value of data is equally critical. First, it preserves national security: leakage of core data (e.g., military or diplomatic information) can threaten state sovereignty [11]. Second, it safeguards public order: large-scale personal data breaches can trigger social unrest — for example, a 2024 data breach in one country led to 100,000 citizens falling victim to telecom fraud [10]. Third, it protects personal privacy: misuse of data can infringe individuals' dignity and degrade quality of life [6].

Unfettered cross-border data flows amplify security risks. Overseas interception can capture foreign governmental data, and data leaks can harm individual rights. China's onshore storage requirement in Article 37 of the Cybersecurity Law is precisely aimed at preventing such risks [1].

4.2.2. Conflicts caused by differing prioritization of values

There are marked differences between developed and developing countries in how they prioritize data values:

1. Developed countries' prioritization: They tend to emphasize economic value, arguing that free cross-border data flows maximize trade benefits and innovation efficiency. Major digital firms in the United States and the EU rely on global data resources for their operations; data localization would directly affect their profits and competitiveness, so these actors generally advocate "economic value first" and oppose strict localization [9].

2. Developing countries' prioritization: They place greater weight on security value. With weaker domestic digital industrial bases and limited technological capacity, developing countries may be less able to cope with the security risks of liberalized data flows. Moreover, localization can protect nascent domestic industries and foster local data markets; therefore, these countries tend to endorse "security value first" and reserve the right to implement localization measures [5,11].

These divergent value priorities produce a stalemate in international rule-making: developed countries push for rules banning data localization [4,9], while developing countries insist on the sovereign right to adopt localization [5,11]. Such polarization makes it difficult to reach a common international position and intensifies conflicts between data localization measures and international trade rules [3].

5. Coordinating pathways for trade regulation conflicts in data localization measures

5.1. Establishing the applicability of the "technology-neutral" principle

5.1.1. Connotation and value of the "technology-neutral" principle

The core of the "technology-neutral" principle is that data regulation measures should not favor specific technologies or service models; instead, they should be guided solely by the objective of achieving policy goals while minimizing trade restrictions [7]. For example, if data encryption or security assessment techniques can achieve the same security effect as localization, onshore storage should not be mandated.

The value of this principle lies in two aspects: Ensuring fair competition: It prevents trade barriers arising from technological preferences. For instance, companies could be allowed to choose cloud-based storage with encryption instead of being forced to store data on physical servers. Optimizing regulatory efficiency: It reduces compliance costs for enterprises. Small and medium-sized enterprises (SMEs) can rely on technology-based solutions instead of investing heavily in onshore data centers [7].

5.1.2. Legal basis and practical references for the "technology-neutral" principle

GATS provides a legal foundation for technology neutrality. Its non-discrimination principle prohibits discrimination based on technology type, and the necessity principle requires selecting measures that minimally restrict trade. Together, these principles support the application of technology neutrality [3]. For example, a country that only permits physical onshore storage while excluding encrypted cross-border transmission would violate both the non-discrimination and necessity principles.

In regional agreements, TPP Article 14 explicitly incorporates the concept of technology neutrality, requiring members to allow alternative technologies to achieve policy objectives [4]. For instance, in cross-border medical data transfers, a member

country may require internationally standardized encryption rather than mandating onshore storage — offering a practical example of technology-neutral implementation [4].

5.1.3. Practical approaches for China to promote the "technology-neutral" principle

5.1.3.1. Domestic level: improving the technical standards system

Leveraging the Data Security Law, China can formulate a Technical Alternatives Assessment Guide for Data Security, specifying security objectives and evaluation indicators for different data types [11]. For example, cross-border financial data may be secured through any of the following: onshore storage, cross-border encryption with real-time monitoring, or third-party certification. Enterprises can choose freely without mandatory localization. Furthermore, the technical catalog should be dynamically updated to include emerging technologies such as blockchain and zero-trust architecture, ensuring that regulation keeps pace with technological development [11].

5.1.3.2. Bilateral level: conducting technical mutual recognition cooperation

Priority can be given to establishing technical mutual recognition mechanisms with RCEP members and Belt and Road countries. Through Mutual Recognition Agreements on Technical Solutions, encryption standards, evaluation processes, and certification qualifications can be mutually recognized [5]. For instance, a Chinese e-commerce platform using an encryption scheme compliant with Chinese standards can enter the Singaporean market without undergoing redundant evaluations, requiring only certification from Chinese authorities — reducing compliance costs [5].

5.1.3.3. Multilateral level: promoting inclusion in rules

At multilateral platforms such as the WTO and APEC, China and other developing countries can propose incorporating the "technology-neutral" principle into global digital trade rules [7]. Member countries would be required to demonstrate the lack of viable alternative technologies before imposing localization measures, publicly disclose approved technical solutions, and accept supervision — thereby preventing disguised trade protection [7].

5.2. Improving the "principle plus exceptions" rule framework

5.2.1. Core logic of the "principle plus exceptions" framework

This framework takes "free cross-border data flow" as the principle and "data localization as the exception". Its core logic is that data should, by default, flow freely, and localization is only allowed under specific legal circumstances. The scope and procedures for exceptions are strictly controlled, achieving a balance of "freedom as the norm, exception as the exception" [12].

This approach both ensures smooth development of digital trade and reserves policy space for national security and privacy protection, avoiding the drawbacks of a one-size-fits-all approach. It is considered the optimal strategy to coordinate conflicts arising from data localization measures [12].

5.2.2. Clarifying the legal scope of exceptions

National Security Exceptions: Limited to situations "involving core national interests", including military data, nuclear facility data, and state secrets. These are to be included in a "National Security Data Directory" and made public. Ordinary commercial data must not be included under this exception [11].

Public Order Exceptions: Limited to "urgent and significant situations", such as pandemic prevention data or major disaster emergency data. Measures must be temporary, automatically expiring within one month after the crisis is resolved, preventing long-term retention [13].

Personal Privacy Exceptions: Applicable only to sensitive personal information (e.g., biometric data, medical data, information of minors). Before localization, alternative measures like data anonymization or de-identification must be evaluated; if alternatives are feasible, localization is not permitted [6].

5.2.3. Establishing legitimate procedures for exceptions

Transparency Obligations: Before implementing localization exceptions, member states must publicly disclose through the WTO or relevant regional secretariats the legal basis, scope, duration, and exemption conditions at least 30 days in advance, giving enterprises time to prepare. Any adjustment of measures must be pre-notified with justifications [3,5].

Consultation Mechanism: A "Data Regulation Consultation Committee" should be established within regional agreements to review whether exception measures comply with the "necessity principle" [13]. If a member state believes another country's measure exceeds the exception scope, it may request consultations. The committee shall issue an evaluation report within 60 days. If consultation fails, dispute settlement mechanisms can be used, ensuring exception measures are compliant [13].

5.3. Promoting rule alignment in regional trade agreements

5.3.1. Establishing unified standards for data classification and tiering

Together with RCEP member states, a "Regional Data Classification and Tiering Guide" should be developed to unify definitions of sensitive, important, and general data [5]:

(1) Sensitive Data: Biometric data, medical records, information on minors, etc., requiring onshore storage or multi-department assessment before cross-border transfer [5].

(2) Important Data: Financial transaction data, energy supply data, etc., allowed to leave the country after a single-department assessment [5].

(3) General Data: Corporate product information, non-sensitive personal data, etc., freely flowing across borders [5].

A unified standard allows enterprises to classify data according to a single framework regionally, reducing compliance costs and minimizing rule conflicts [13].

5.3.2. Building mutual recognition mechanisms for cross-border data flow

Mutual Recognition of Assessment Bodies: Establish a "Regional Data Security Assessment Agency Certification Committee" to review third-party agencies' qualifications. Agencies compliant with ISO/IEC 27701 standards are included in the mutual recognition list, and their reports are valid regionally, eliminating redundant assessments for enterprises [13].

Unified Assessment Indicators: Develop "Regional Data Security Assessment Indicators", specifying core metrics such as encryption strength, risk monitoring, and emergency response, ensuring consistency in evaluation outcomes [13]. For example, cross-border financial data must use AES-256 encryption and implement a 72-hour emergency response plan.

Traceability of Assessment Results: Create a regional unified database where mutual recognition agencies upload assessment reports. Member state regulators can query and verify the reports, and any falsification leads to revocation of agency qualifications, ensuring credibility and integrity of evaluations [13].

6. Conclusion

6.1. Core findings

Data localization measures exhibit a dual attribute of being both a "legitimate public policy" and a "measure affecting trade in services." This duality places them in a tension between national sovereignty and trade freedom, generating conflicts with GATS principles of market access, non-discrimination, and rules under various regional trade agreements [3,4,5,9].

The root causes of these conflicts lie in: Differences in data governance models — the U.S., EU, and China each prioritize different aspects of governance [6,9,11]. Divergent prioritization of data values — developed countries emphasize economic value [9], while developing countries emphasize security value [5,11]. These differences make it difficult to achieve unified international rules [3].

Resolving these conflicts requires a three-dimensional approach: technical neutrality + principle-plus-exception + regional alignment. Technical neutrality prevents technology-based discrimination [7]; principle-plus-exception clearly defines the boundaries of permissible measures [12]; and regional alignment reduces the cost of fragmented rules [13]. Together, these approaches achieve a balance of security and freedom.

6.2. Practical recommendations for China's participation in international rule-making

Domestic Level: Refine data classification and tiering; issue a "Data Localization Implementation Guide", applying localization only to core and important data [11]. Accelerate the development of data security technical standards, incorporating technologies such as zero-trust architecture and federated learning into the recognized framework [11].

International Level: Within the RCEP framework, promote unified data classification and mutual recognition of assessments to establish a "regional demonstration model" [5]. In WTO negotiations, collaborate with developing countries to incorporate technical neutrality and principle-plus-exception into multilateral rules [7,12], and oppose unilateral clauses [9]. Engage in technical mutual recognition with the EU and ASEAN to reduce rule discrepancies [5,6].

6.3. Research limitations and future directions

This study has two main limitations: It does not analyze WTO dispute settlement cases to evaluate the practical application of rules [3]. It lacks in-depth examination of emerging data types, such as AI training data and blockchain data, in the context of localization regulations [10]. Future research can be deepened in three directions: Analyze WTO cases to assess legal standards for data localization [3]. Explore regulatory approaches for emerging data types [10]. Quantitatively evaluate the impact of data localization on digital trade [10], providing empirical support for rule-making [7].

References

[1] Standing Committee of the National People's Congress of the People's Republic of China. (2016). Cybersecurity Law of the People's Republic of China [Z]. Beijing: China Legal Publishing House.
[2] Parliament of the Commonwealth of Australia. (2012). Personally Controlled Electronic Health Records Act (PCEHR) [Z]. Canberra: Commonwealth of Australia Publishing Service.
[3] World Trade Organization. (1994). General Agreement on Trade in Services (GATS) [Z]. Geneva: World Trade Organization.
[4] New Zealand Government. (2016). Trans-Pacific Partnership Agreement (TPP) [Z]. Auckland: New Zealand Government.
[5] Association of Southeast Asian Nations Secretariat. (2020). Regional Comprehensive Economic Partnership Agreement (RCEP) [Z]. Hanoi: ASEAN Secretariat.
[6] European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data [Z]. Brussels: European Union Official Journal.
[7] Reed, C. (2022). The role of technical neutrality in digital trade agreements. *Journal of International Economic Law*, 25(1), 45–68.
[8] State Council of the People's Republic of China. (2013). Regulations on the Administration of Credit Reporting Industry [Z]. Beijing: China Legal Publishing House.
[9] United States Trade Representative. (2018). United States-Mexico-Canada Agreement (USMCA) [Z]. Washington, D.C.: Office of the United States Trade Representative.
[10] China Academy of Information and Communications Technology. (2024). China Digital Trade Development Report (2024) [R]. Beijing: China Academy of Information and Communications Technology.
[11] Standing Committee of the National People's Congress of the People's Republic of China. (2021). Data Security Law of the People's Republic of China [Z]. Beijing: China Legal Publishing House.
[12] Wang, G. (2022). Legal regulation of digital trade. *China Legal Science*, (3), 132–150.
[13] Liu, S. (2023). Conflicts and coordination of cross-border data flow rules in regional trade agreements. *Modern Law Science*, (2), 178–192.