Proceeding of ICGPSH 2025 Symposium: International Relations and Global Governance
DOI: 10.54254/2753-7048/2025.BO23772

Fragmented Rules, Global Flows: How Legal Differences Shape the Cross-Border Data Landscape - Evidence from the EU, US, and China

Shanglin Jiang

Law School, Washington University in St. Louis, St. Louis, USA
j.shanglin@wustl.edu

Abstract: The exchange of data across borders has become crucial for international commerce and technological progress. However, major differences in privacy principles and regulatory systems among China, the United States, and Europe have led to fragmented global data governance. This paper examines whether such institutional differences hinder the global economy. Through analysis of cases including Meta, TikTok, Microsoft, and Apple-Google, the study finds that these differences create data barriers, raise compliance costs, and limit cross-border collaboration. To address this, the paper proposes a multi-level coordination framework—international, regional, and national—to achieve equilibrium in data autonomy and international data exchange.

Keywords: data privacy, cross-border data, regulatory divergence, global governance, legal harmonization

1. Introduction

Information is the lifeblood fueling economic growth across the globe in the modern era, and international data exchanges serve as a crucial conduit for fostering connections between nations in the realms of commerce, finance, tech innovation, and social engagement. Despite the rising significance of transnational data in worldwide economic expansion, in recent years, numerous nations globally have enacted stringent laws for safeguarding data privacy, to build a data governance system centered on sovereignty, security and rights protection, resulting in inconsistent rules and standards across the international community, and heightened constraints regarding unrestricted international data flow.

In particular, under the EU's General Data Protection Regulation (GDPR) [1], China's Personal Information Protection Law (PIPL) [2], and the U.S. data regulation systems, the legal frameworks, compliance processes, and risk evaluations vary considerably for international data transfers. As Yamada mentioned, this divergence and restrictions not only exacerbate the cost of data compliance for enterprises globally, but also may have a substantial impact on SMEs, biotechnology, artificial intelligence, and other areas that are highly dependent on data sharing [3].

This study investigates the effects of EU, US and China data privacy frameworks on the global economy from the perspective of comparative law, and to explore possible paths for institutional harmonization. By examining typical jurisprudence and policy changes, this paper aims to answer a central question: do these institutional differences constitute “data barriers” in the growth of the

DOI: 10.54254/2753-7048/2025.BO23772

digitalized global economy? If so, what strategies can be used to achieve harmonization and compatibility between the different systems?

2. Thesis and road map

The basic proposition of this paper is that, although transnational data exchanges are essential for driving international commerce and technological progress, today's legal frameworks worldwide remain fundamentally fragmented and misaligned, as evidenced by the inconsistent interpretations and applications of key principles like "data sovereignty," "individual privacy rights," and "state security concerns." This patchwork of conflicting approaches creates a disjointed framework where fundamental concepts lack universal clarity or implementation. This fragmentation not only exacerbates compliance uncertainty for enterprises, but also reduces the efficiency of global digital economy cooperation. This article argues that the world currently lacks a unified and effective governance framework for regulating transnational data movement, and that institutional conflicts between China, the US, and Europe are magnifying this governance gap.

To support this argument, the article is structured as follows: Part IV integrates key scholarly perspectives on international data movement and personal privacy concerns, examining the roots of organizational fragmentation and the shortcomings of current collaborative avenues; Part V clarifies the research methodology and hypothetical framework; Part VI examines the specific impacts of institutional differences on firms and markets via case studies from the EU, US, and China; Part VII puts forward multi-level coordination proposals on this basis, covering international soft law mechanisms, regional cooperation paths and optimization of domestic legislation; Part VIII summarizes the whole paper and looks forward to the future development direction of global data governance.

3. Literature review

3.1. The value and challenges of transnational data flows

Lately, international data exchange stands as a crucial element underpinning the worldwide digital economic landscape, a characterization by Voss as "the signature of 21st-century globalization." [4] He also notes that it's supportive of global business activities and innovation. Given the rapid advancement of IoT technology, data volume and flow rates are increasing dramatically, providing a powerful impetus for SMEs to expand their global markets and improve the quality of their digital services.

However, this wide circulation of data also raises new governance challenges. Mattoo and Meltzer point out that online financial, health, education, and communication services often depend on the mass gathering and analysis of individual-level data [5]. When sensitive information is shared with nations that have weaker privacy regulations, it can compromise the data protection goals of the originating country, creating potential legal and regulatory pitfalls. Sullivan, by contrast, highlights on the large amount of sensitive information generated by IoT devices in the course of their ongoing operation, arguing that this exacerbates the privacy risks related to transnational data exchange [6].

3.2. Regulatory divergence and institutional conflict

Global data governance shows a clear pattern of institutional differentiation. The EU, with the GDPR at its core, has established the position that privacy is recognized as an essential human right, emphasizing individuals' authority over their own data and the requirement of "adequacy" for worldwide data movement. The U.S., conversely, embraces a consumer-focused framework in which data privacy is predominantly considered a customer entitlement and emphasizes corporate self-

DOI: 10.54254/2753-7048/2025.BO23772

regulation. On this basis, the CLOUD Act broadens legal access to international data, igniting debates on jurisdictional reach. China bolstered data sovereignty safeguards and national security measures through legislation such as the National Security Law (NSL) [7], the Cybersecurity Law (CSL) [8], the Data Security Law (DSL) [9], PIPL, and has created a strict mechanism for assessing data localization and exit.

The differences between these models are not only philosophical, but also reflect the trend of "institutional fragmentation" in the path of implementation. Yik-Chan and Zhao argue that the inconsistency of regulatory policies across countries is the biggest source of risk facing the digital economy [10]. They point out that although regional agreements such as the CPTPP provide a buffer mechanism to some extent, due to geographic constraints and divergent national interests, it is difficult for these agreements to solve the problem of institutional harmonization at the global level. Voss even describes the current state of affairs as a "splintered Internet" and warns of the potential for impeded digital innovation, reduced economic efficiency, and limited freedom of expression.[4]

In addition, Burri criticizes accords like CPTPP, USMCA, and the EU-US Privacy Shield for failing to reconcile regulatory enforcement with individual data protection goals, thereby heightening uncertainty about the application of the law [11]. Laidlaw highlights the trend where national data privacy laws are increasingly stepping out of sync with the rapid evolution of global trade deals, which could further splinter the international governance of data [12].

3.3. Existing academic approaches to coordination

To address institutional frictions in cross-border data flows, existing studies have suggested harmonization paths from multiple perspectives, covering areas such as soft law mechanisms, trade agreements, human rights protection and market competition.

At the global level, Yik-Chan and Zhao suggest constructing an inclusive, proportional, and hierarchical soft law framework through platforms such as the WTO and setting a minimum standard of consistency while respecting sovereign diversity [10]. Mattoo and Meltzer highlight the contentious nature of the EU-US "Privacy Shield" agreement, yet they argue that its framework for reciprocal certification recognition can provide insights for institutional harmonization and advocate its extension to more countries [5].

On trade paths, Casalini and López González contend that data-related provisions should be integrated into free trade agreements to ensure transparent, non-discriminatory, and minimally trade-restrictive policies [13], while Burri argues that FTAs can serve as "laboratories" for institutional innovation. The convergence of standards between different governance systems can be gradually promoted [11].

Laidlaw suggests treating data privacy as an essential component of the global human rights issue, so as to balance trade facilitation and rights protection [12], while Chen et al. suggest strengthening competition policy in the digital market at the global level, and constructing a policy oriented to "free data flow" [14].

3.4. Research gaps and problem framing

Although existing studies have put forward theoretical analyses and policy recommendations on global data governance from different perspectives, there are still two deficiencies: first, most of them focus on normative discussions and lack empirical analyses based on typical jurisdictions; and second, Current analyses tend to overlook the complex institutional dynamics between China, the U.S., and the EU, failing to adequately address how these geopolitical relationships influence the smooth operation of international data transfers and they lack the systematic design of cross-jurisdictional comparisons and coordinating mechanisms.

DOI: 10.54254/2753-7048/2025.BO23772

In order to make up for the above shortcomings, this paper analyzes and compares legal frameworks and representative case studies of three jurisdictions to examine whether the institutional differences constitute "data barriers" and seeks integrated global, regional, and domestic strategies to address escalating institutional divisions.

4. Methodology and hypotheses

This paper adopts a comparative methodology to analyze the data privacy regulatory regimes of three major jurisdictions, namely the EU, the U.S., and China, in international data transit, combining them with typical cases to assess whether the different regimes constitute barriers in the global digital economy, and to further explore possible paths for institutional harmonization and rule convergence.

The core research question of this paper is: Do US, EU, and Chinese data privacy law variations genuinely impact the international financial system? If so, how should institutional harmonization and rule convergence take place?

Around this question, this paper proposes the following two sets of opposing research hypotheses:

H1: Differentiated data privacy regimes pose no major threat to worldwide financial systems.

H2: Differentiated regimes do create "data barriers" and pose challenges to the evolution of a worldwide online marketplace.

H2a: Varying regulations raise business compliance expenses;

H2b: Firms often process data locally given varying regulations, hindering international collaboration;

H2c: Fragmentation of regimes delays data flows and affects operational efficiency.

5. Case studies

In order to test the research hypothesis put forward in this paper, i.e., whether the differences in data privacy rules among different countries constitute data barriers in the global economy, this paper selects three representative data governance jurisdictions of the EU, the U.S., and China, and analyzes the operating logic of the current system in practice and its real-world impacts, starting from their institutional arrangements and typical cases, respectively.

5.1. The EU: unified high standards and human rights-oriented regulation

The EU's data safeguards rest on privacy, a cornerstone of human rights. Since the 1981 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108), the European Union has laid the groundwork for the legal governance of international data transfers [15]. As Xu highlights, the European Council's primary focus during this time was on tackling the obstacles to data flow resulting from the varied national regulations of Member States [16]. Their goal was legal solutions fostering open data exchange across Europe's single market. The 1995 Directive 95 /46 /EC clarified for the first time the "principle of adequacy", mandating equivalent data protections from non-EU nations prior to EU data access [17]. In 2016, the EU introduced GDPR to standardize data protection laws, enhance transparency, and strengthen individuals' control over personal information collection and usage, while also giving data supervisors strong enforcement capabilities. The broad extraterritoriality of Article 3 of the GDPR makes it mandatory for non-EU companies to comply with its high standards even if they operate outside the EU. Article 45 establishes clear guidelines for international transfer of individual data beyond EU borders, permitting exchanges only when the European Commission officially recognizes that the recipient jurisdiction maintains privacy safeguards equivalent to those within the Union—a designation commonly referred to as an "adequacy decision." In 2023, the adoption of the Regulation

DOI: 10.54254/2753-7048/2025.BO23772

on Harmonised Rules on Fair Access to and Use of Data (Data Act) enhances safeguards for transferring global non-personal information and affirms the EU's data economy dominance [18].

Against this backdrop, Meta has become a landmark case in the implementation of the GDPR regime. In *Schrems I* [19] and *Schrems II* [20], the European Court of Justice (ECJ) twice held that US-EU data transfer agreements (Safe Harbor and Privacy Shield) did not satisfy the "adequacy" requirement, which ultimately led to their invalidation. The Court highlighted American government's approach to accessing data failed to meet "necessity and proportionality" criteria and the absence of adequate judicial protection for EU citizens within the U.S. In 2023, despite Meta's adoption of a revised set of Standard Contractual Clauses (SCCs) authorized by the European Commission—alongside supplementary safeguards—the Irish Data Protection Commissioner determined these steps still fell short of adequately protecting individuals' core rights and freedoms from potential risks [21]. As a result, Meta faced a hefty €1.2 billion penalty from the governing body and was required to cease data transfers and processing. This case highlights the institutional logic of the EU's high standards of privacy regulation, but also raises concerns about its negative externalities. As Okenyi points out, overly stringent data privacy regimes can be counterproductive, even undermining the very social well-being they are intended to enhance [22]. For example, large fines would not only weigh heavily on large tech firms, but also force some SMEs to exit the European market due to the high cost of compliance, undermining market vitality and digital innovation. Simultaneously, severe restrictions on data transfer may also hinder information sharing in areas such as finance, healthcare, technology, etc., with associated social impacts, including reduced quality of services, increased unemployment, and limited access to public communication channels.

Therefore, although the EU has established a rigorous international data privacy framework anchored in human rights, in terms of real-world effects, as the hypotheses in this study suggest (H2a, H2c), the system significantly increases the compliance burden of enterprises on the one hand, while also hindering international data transfers due to legal ambiguities, thus affecting the operational efficiency of enterprises.

5.2. The U.S.: balancing free flow and security in data governance

The United States, in contrast to the EU, refrains from considering data protection as an inherent and universally recognized human entitlement. Instead, its focus is more on market efficiency and business interests and regulates privacy within a consumer protection framework. The United States has yet to establish comprehensive federal privacy laws, leaving protections fragmented across various sectors like healthcare, online activity, and minors' data. Instead, states have stepped up—with legislation such as California's CCPA leading the charge—creating a patchwork of regulations rather than a cohesive national standard. Amid escalating transnational data exchange, the U.S. relies on bilateral agreements (e.g., Safe Harbor, Privacy Shield) with the EU and other regions to build compliant transmission mechanisms. Meanwhile, the U.S. champions unhindered data transfer across international boundaries via diverse trading agreements – including the TPP, CPTPP, and USMCA, and has used APEC to promote the CBPR system to strengthen its ability to export its system for global data governance.

Although the U.S. system is designed to be market-oriented and free-flowing, under certain circumstances, particularly in matters of national security and law enforcement, its governance logic emphasizes "security prioritization" and "jurisdictional expansion." This "internal division" of the system is particularly evident in the following typical cases.

In *United States v. Microsoft Corp*., the DOJ, citing the Stored Communications Act (SCA), sought access to Microsoft's user email data stored on Irish servers [23]. Microsoft contended the data resided beyond national borders and that the U.S. warrant of search was inapplicable. The appeal reached the Federal Supreme Court, yet the case was terminated during the hearing process after the U.S. passed

DOI: 10.54254/2753-7048/2025.BO23772

the CLOUD Act in 2018, which grants police departments permission to retrieve data held by U.S.-based entities offshore. The case exposed the limitations of traditional law in global data forensics, and also reflected the trend of the United States to expand its "long-arm jurisdiction" through legislation, further raising the issue of international data sovereignty and judicial conflict.

In addition, the TikTok case exemplifies the tension between data governance and national security. Since 2020, U.S. officials have been breathing down ByteDance's neck, demanding the company relinquish its control over TikTok's U.S. operations. Fueled by concerns that the Chinese government might get its hands on Americans' personal data, they've also made repeated attempts to hamstring the app through legislation. TikTok has subsequently pursued the data localization strategies of Project Texas and Project Clover in the U.S. and the European Union to ease regulatory pressure by moving user data to domestic servers. Although this compliance strategy helps maintain short-term operations, it also deepens the global fragmentation of data governance, creating more regulatory divides and isolated data systems. In addition, Campbell argues that addressing cybersecurity and privacy concerns by blocking a particular app is a costly game of whack-a-mole with limited results [24]. Governments should instead pinpoint key vulnerabilities and bolster privacy/security benchmarks for digital platforms and application distributors to better counter prospective hazards.

In summary, while the United States promotes free data transfers, it also tightens control through national security concerns, long-arm jurisdiction, and the export of its own regulatory standards. Although this dual-track institutional path enhances the country's external data sovereignty, it also exacerbates institutional conflicts and compliance frictions in the global governance environment, further confirming the H2 hypothesis: institutional divergence and fragmentation have become the key obstacles to global data flows, especially for multinational enterprises, bringing continuous compliance uncertainty and operational pressure.

5.3. China: a data localization-driven governance model rooted in sovereignty and security

China's data management framework prioritizes "data jurisdiction" and "national protection," focusing on oversight of crucial data assets. Through four core laws, namely NSL, CSL, DSL and PIPL, China has built a relatively complete framework for controlling localization and cross-border transmission. Among them, Article 8 of the NSL emphasizes the "overall concept of national security," which covers both domestic and international stability, public safety, civilian and military protection, as well as non-traditional threats. According to Article 37 of the CSL, entities managing key information are mandated to localized the storage of personal information within the country, while DSL Article 31, along with PIPL Articles 38 & 40, mandate stringent prerequisites for international data exchange, such as security evaluations, authentication, and standard contracts. This series of laws establishes a "precautionary" licensing system for governing outbound data transmission and strengthen national sovereignty in cyberspace.

At the practical level, Apple has responded to policy requirements since 2017 by signing an iCloud strategic cooperation agreement with the Guizhou Provincial Government and deciding to build its first data center in mainland China, with an investment of up to $1 billion, which will be operated and managed by Guizhou on the Cloud for storing photos, videos, documents and other personal information of users in mainland China to ensure compliance with the CSL, DSL and other legal requirements for data localization. While this move improves data compliance, it also directly restricts the flow of data across borders, forcing Apple to adjust its global data architecture, increasing operating costs and potentially undermining the efficiency of its data sharing and system collaboration around the world.

Similarly, Google expanded its operations into China by introducing a region-specific version of its search platform (google.cn). However, Google exited China in 2010 after refusing to comply with local search result censorship mandates. In addition, in 2021, LinkedIn and Yahoo both exited the

DOI: 10.54254/2753-7048/2025.BO23772

Chinese market due to more challenging operating environments and higher compliance requirements. Their withdrawal not only reflects the legal and ethical dilemmas of multinationals in dealing with content censorship, but also stems largely from China's mandatory requirements for localized data processing and compliance control. This example further illustrates how data localization policies are forcing companies at the institutional level to reorganize their global business structure or even choose to abandon the market in order to avoid compliance risks.

In the face of a tightening regulatory environment, global companies have adopted data localization strategies to address compliance risks. Heightened data protection, conversely, restricts adaptable international data sharing. Bauer notes that localization may lead to a decline in productivity in data-intensive industries [25]; Lu criticizes its potential misuse to restrict the flow of information and expand surveillance powers [26]. This trend also exacerbates institutional frictions in global governance, putting developing countries at a disadvantage in the rules game.

Therefore, while China's data governance model strengthens security boundaries and enhances national sovereignty, it also objectively exacerbates the institutional friction of global data governance and pushes up the operational and compliance costs of enterprises. This confirms the H2 hypothesis proposed in this paper: institutional differences and data localization measures are constituting "data barriers" that weaken the efficiency of global data sharing and collaboration—especially within highly interconnected global digital supply chains—posing serious challenges to multinational corporations.

The institutional differences between the three models, from the EU's uniform protection, to the US's free-flow-oriented but security-constrained approach, to China's localization-based control, not only construct three different cross-border data compliance frameworks, but also form a de facto "global data barrier". As suggested in the second hypothesis (H2) of the paper, these disparities truly hinder effective global digital partnerships and data-driven advancements. They also impede unrestricted international data movement across global markets through mechanisms such as increasing compliance costs, encouraging localization, and delaying data flow. These cases not only confirm the problem of "governance fragmentation" brought about by institutional differences, but also provide the institutional background and practical basis for the global coordination mechanism proposed later.

6. Recommendations

The obvious differences in the concepts and rule designs of data governance among the three major jurisdictions of Europe, the United States and China have spawned enduring systemic clashes in worldwide data oversight, defying simple, unitary solutions. Based on the previous case study, this study proposes collaborative recommendations for global, regional, and domestic implementation: to promote the consensus on basic rules at the global level, to strengthen the institutional articulation at the regional level, and to improve the legislative details at the domestic level. Through this three-tier structure, it is hoped that a more pragmatic balance can be found between data sovereignty, national security and cross-border flow, providing a feasible solution to break the "data barrier".

6.1. International level: aligning core rules and building platforms for cooperation and dispute settlement

Currently, disparities exist across nations in data jurisdiction, confidentiality safeguards, and international data exchanges, and there is a lack of articulation between the regimes, resulting in enterprises facing duplicative compliance and rising costs in different countries, and resulting impediments to international data exchange. Considering the different institutional backgrounds and interests of different countries, it is not realistic to harmonize mandatory global laws in the short term.

DOI: 10.54254/2753-7048/2025.BO23772

Comparatively speaking, it is more feasible to start with "soft law" mechanisms to promote cooperation through some basic principles and flexible mechanisms.

According to Ao, although existing mechanisms such as OECD's privacy framework and APEC's international data protection regulations provide an initial framework for data flow, they still have problems such as weak legal effect, limited applicability to countries, and incompatibility of standards [27]. For example, the CBPR system is not yet formally recognized by the EU, resulting in the need for many companies to repeatedly apply for certification in different regions. On the basis of these existing mechanisms, it is suggested that OECD, WTO or an agency under the United Nations take the lead in promoting the formation of a global minimum standard that includes basic principles such as necessity, proportionality and transparency. It is also possible to promote the establishment of a mutual recognition mechanism for standards, so as to help enterprises realize one-time certification and multi-location application among different countries.

Besides the rules themselves, there should also be a platform for cooperative dialog. Reference can be made to the experience of the Internet Governance Forum (IGF) to set up a "Global Data Governance Forum" or a "Digital Economy Cooperation Conference". The forum should involve governments, technology enterprises, civil society and academia, and hold regular consultations on data issues, especially encouraging the participation of developing countries and nongovernmental organizations, so as to prevent the rules from being dominated by a small number of countries.

In addition, mechanisms should be set up to deal with disputes. Currently, there is a lack of neutral and fair channels for resolving conflicts over cross-border data, which can easily escalate technical issues into political ones. An arbitration mechanism for cross-border data disputes can be established by drawing on the experience of international commercial arbitration, with an independent third party solving the problem and guaranteeing fairness and efficiency.

Taken together, the multi-pronged approach, ranging from minimum standards and mutual recognition mechanisms to cooperation platforms and dispute resolution mechanisms, will help to promote the accumulation of consensus while respecting the differences in the systems of various countries, and provide a more stable and fairer cooperation framework for global data governance.

6.2. Regional level: bridging U.S.-EU-China data rule gaps through flexible collaboration

Significant disparities exist in the legal frameworks governing data management within the EU, the U.S., and China. The EU emphasizes privacy as a fundamental right, enforcing stringent safeguards; the U.S. places more emphasis on market autonomy and corporate flexibility; and China focuses on national security and control of critical data. Divergent organizational doctrines fuel recurrent U.S., China, and Europe clashes concerning international data transfer, intensifying corporate compliance demands.

If achieving globally consistent regulations proves challenging in the near future, regional collaboration could serve as a valuable alternative for fostering communication and reciprocal recognition between these three legal systems. For instance, the European Union has deemed Japan's data transfer to Europe as adequate, facilitating unrestricted data exchange. By adjusting the laws and setting up additional safeguards, the two sides reached mutual recognition of data under different systems. China and Europe can look to this model and explore similar paths of cooperation while respecting their respective laws.

China and the U.S., despite their differences, can also start with less sensitive areas to promote technical cooperation. For example, the "modularization" strategy of DEPA is ideal for fostering trust in sectors like AI, international online trade, and cloud computing, with the potential to broaden the horizons of collaboration down the line.

In addition, the practice of RCEP also provides useful experience in regional cooperation. As Zhang pointed out, the agreement not only encourages cross-border flow of data, but also reserves

DOI: 10.54254/2753-7048/2025.BO23772

reasonable regulatory space for member countries through provisions such as the "necessity principle" and "public policy exceptions" [28]. Recent China-ASEAN digital economy collaboration follows a "step-by-step, phased integration" approach, which builds a feasible transition mechanism between countries with large differences in systems.

Through flexible cooperation and progressive mutual recognition arrangements at the regional level, countries with significant institutional differences, such as China, the United States and Europe, are expected to reach a consensus in some areas first, thus laying the foundation for future harmonization of a wider range of systems and the integration of global rules.

6.3. National level: refining data localization with flexible rules for both security and openness

Against the backdrop of strengthening data security and sovereignty protection, many countries have established relatively strict data localization and cross-border regulatory regimes to govern critical national information's storage, transfer, and application. However, amid growing global data exchanges, strict localization rules present fresh challenges: enterprises face higher compliance costs for cross-border operations, cross-border cooperation is less efficient, and institutional conflicts between different jurisdictions have become more prominent.

To harmonize safeguards and accessibility, it is recommended that when formulating localization policies, countries should introduce a classification and grading management approach, and categorize data as "key," "important," or "general" based on the criteria of data sensitivity and usage scenarios, respectively, using different cross-border processing requirements. For example, "key data" may retain strict local storage obligations, while "important data" may be allowed to leave the country after completing a security assessment or obtaining certification, and "general data" should be subject to a more simplified cross-border regime. In 2024, China released a guideline on data classification and grading, which explicitly defines "key data" as important information that may endanger national interests, disrupt the economy, or threaten public security if leaked, while general business data does not fall within the scope, and more flexible cross-border mechanisms can be applied [29].

At the same time, certain flexible exception mechanisms can be established, such as the introduction of a "compliance white list" system, which provides incentives such as simplified assessment procedures and prioritized approval permissions for enterprises with good compliance records in cross-border operations; the establishment of a "free trade zone data pilot", which facilitates the investigation of adaptable data movement regulations across borders in a designated area. Such mechanisms not only help to reduce the burden on enterprises, but also facilitate the accumulation of practical experience in regulation and the optimization of policy design.

In addition, when formulating data localization policies, countries should also give full consideration to their impact on international cooperation, so as to avoid unnecessary conflicts resulting from unilateral expansion. In the design of the legal system, emphasis should be placed on compatibility with international cooperation frameworks, and a mechanism for transformation from domestic regulation to offshore compliance should be gradually established. This more adaptable approach to localization policies aims to encourage a balanced international exchange of data, all while respecting each nation's right to govern its own information. The hope is that it will also boost cooperation and make global digital economies more compatible with each other institutionally.

7. Conclusion

With the digital terrain constantly changing, the transboundary flow of information stands as a pivotal factor in international collaboration, but the institutional differences in data sovereignty, privacy and

DOI: 10.54254/2753-7048/2025.BO23772

security among countries are becoming more and more prominent, bringing challenges in governance coordination.

This paper verifies that institutional differences constitute “data barriers”, which increase compliance costs and weaken data flow efficiency through institutional comparisons and typical case analyses of three major jurisdictions, namely the EU, the US, and China. In order to alleviate the tension between the three governance paradigms, this paper advocates for advancing regulatory alignment and refining governance strategies across global, regional and national dimensions, so as to achieve a more sustainable balance between security and openness.

In summary, international data oversight should move beyond institutional competition toward collaborative consensus-building across disparate regulatory frameworks. Creating an open, secure, and interoperable data exchange framework is essential for unlocking the global digital economy's potential.

References

[1] *European Parliament and Council. General Data Protection Regulation (GDPR), Regulation (EU) 2016/679. Official Journal L 119, April 27, 2016.*

[2] *National People’s Congress Standing Committee of the People’s Republic of China. Personal Information Protection Law of the People’s Republic of China. Adopted August 20, 2021, effective November 1, 2021.*

[3] *Yamada, Hideo. 2022. “Data Is the Lifeblood of the Global Economy. But Restrictions on Cross-Border Data Flows Are Now a Reality.” United Nations University, October 6. https://unu.edu/article/data-lifeblood-global-economy-restrictions-cross-border-data-flows-are-reality.*

[4] *Voss, W. Gregory. 2020. “Cross-Border Data Flows, the GDPR, and Data Governance.” Washington International Law Journal 29 (3): 485–514. https://digitalcommons.law.uw.edu/wilj/vol29/iss3/7.*

[5] *Mattoo, Aaditya, and Joshua P. Meltzer. 2018. “International Data Flows and Privacy: The Conflict and Its Resolution.” Journal of International Economic Law 21 (4): 769–789. https://doi.org/10.1093/jiel/jgy044.*

[6] *Sullivan, Clare. 2019. “EU GDPR or APEC CBPR? A Comparative Analysis of the Approach of the EU and APEC to Cross-Border Data Transfers and Protection of Personal Data in the IoT Era.” Computer Law & Security Review 35 (4): 380–397. https://doi.org/10.1016/j.clsr.2019.05.004.*

[7] *National People’s Congress of the People’s Republic of China. National Security Law of the People’s Republic of China. Adopted July 1, 2015.*

[8] *National People’s Congress of the People’s Republic of China. Cybersecurity Law of the People’s Republic of China. Adopted November 7, 2016, effective June 1, 2017.*

[9] *National People’s Congress Standing Committee of the People’s Republic of China. Data Security Law of the People’s Republic of China. Adopted June 10, 2021, effective September 1, 2021.*

[10] *Chin, Yik-Chan, and Jingwu Zhao. 2022. "Governing Cross-Border Data Flows: International Trade Agreements and Their Limits" Laws 11, no. 4: 63. https://doi.org/10.3390/laws11040063*

[11] *Burri, Mira. 2021. “Data Flows versus Data Protection: Mapping Existing Reconciliation Models in Glo bal Trade Law.” In Law and Economics of Regulation, edited by Michael Faure, 129–158. Cham: Sprin ger. https://doi.org/10.1007/978-3-030-70530-5_7.*

[12] *Laidlaw, Emily. 2021. “Privacy and Cybersecurity in Digital Trade: The Challenge of Cross-Border Data Flows.” SSRN Scholarly Paper No. 3790936. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3790936.*

[13] *Casalini, F., and J. López González. 2019. “Trade and Cross-Border Data Flows.” OECD Trade Policy Papers, no. 220. Paris: OECD Publishing. https://doi.org/10.1787/b2023a47-en.*

[14] *Chen, Lurong, Wallace Cheng, Dan Ciuriak, Fukunari Kimura, Junji Nakagawa, Richard Pomfret, Gabriela Rigoni, and Johannes Schwarzer. 2019. The Digital Economy for Economic Development: Free Flow of Data and Supporting Policies. Policy Brief 4, Task Force 8: Trade, Investment and Globalization, T20 Japan 2019. https://ssrn.com/abstract=3413717.*

[15] *Council of Europe. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108). Strasbourg, January 28, 1981.*

[16] *Xu, Duoqi. 2018. “International Pattern of Personal Data Cross-border Flow Regulation and China’s Response.” Legal Forum 33 (3): 130–137. https://doi.org/CNKI:SUN:SDFX.0.2018-03-013.*

[17] *European Parliament and Council. Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. Official Journal L 281, November 23, 1995.*

[18] *European Parliament and Council. Data Act, Regulation (EU) 2023/2854. Official Journal L, December 13, 2023.*

DOI: 10.54254/2753-7048/2025.BO23772

[19] *Court of Justice of the European Union. Maximillian Schrems v Data Protection Commissioner (Schrems I). Case C-362/14, ECLI:EU:C:2015:650. October 6, 2015.*
[20] *Court of Justice of the European Union. Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (Schrems II). Case C-311/18, ECLI:EU:C:2020:559. July 16, 2020.*
[21] *Irish Data Protection Commission. 2023. "Data Protection Commission Announces Conclusion of Inquiry into Meta Ireland." Data Protection Commission, May 22. https://www.dataprotection.ie/en/news-media/press-releases/Data-Protection-Commission-announces-conclusion-of-inquiry-into-Meta-Ireland.*
[22] *Okenyi, Sunday Chinweike. 2024. Meta: The Cost of Strict Data Privacy Regime in the Era of Technology-Driven Economy. August 20. https://ssrn.com/abstract=4971392.*
[23] *United States v. Microsoft Corp., 584 U.S. ___ (2018).*
[24] *Campbell, Natalie. 2025. "The Global Impact of a US TikTok Ban." Internet Society, January 25. https://www.internetsociety.org/blog/2025/01/the-global-impact-of-a-us-tiktok-ban/.*
[25] *Bauer, Matthias, Martina F. Ferracane, Erik van der Marel, and Global Commission on Internet Governance. 2016. "Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization." In A Universal Internet in a Bordered World: Research on Fragmentation, Openness and Interoperability, edited by Centre for International Governance Innovation. http://www.jstor.org/stable/resrep05249.9.*
[26] *Lu, Wenxi. 2024. "Data Localization: From China and Beyond." Indiana Journal of Global Legal Studies 31 (1): 183–202. https://muse.jhu.edu/article/924201.*
[27] *Ao, Haijing. 2022. "Data Protection Through International Soft Law." Jurists Review 39 (2): 158–172. https://doi.org/10.16390/j.cnki.issn1672-0393.2022.02.002.*
[28] *Zhang, Xiao-jun. 2025. "On the Conflict and Coordination of Data Jurisdiction." Politics and Law Review (1): 95–109. https://doi.org/CNKI:SUN:ZFLC.0.2025-01-007.*
[29] *Standardization Administration of China. Data Security Technology — Rules for Data Classification and Grading (GB/T 43697–2024). Beijing: Standards Press of China, 2024.*