International Journal of Advanced Research in Islamic Studies and Education (ARISE) e-ISSN 2785-9088

DATA SOVEREIGNTY AND CROSS-BORDER DATA FLOWS UNDER THE MULTILATERAL GOVERNANCE FRAMEWORK: AN INTERNATIONAL LEGAL APPROACH BASED ON PLATFORM RESPONSIBILITY

LIAO PEIHONG[*1]

[1*] Guagxi University for Nationalities Blockchain Research Institute. No.100, East Daxue Road, Xixiangtang District,Nanning, Guangxi,China.
Corespondent Email: peihongliao94@gmail.com

Received: 24 May 2025 *Accepted: 19 June 2025* *Published: 26 August 2025*

Abstract: In the context of the globalized digital economy, the tension between data sovereignty and cross-border data flows has become increasingly prominent. Building an effective multilateral governance framework has become a crucial issue urgently needed by the international community. This study focuses on exploring an international legal approach centered on platform responsibility, aiming to balance national data sovereignty requirements with the need for global data free flow. Through a comparative analysis of the EU's General Data Protection Regulation (GDPR), China's Data Security Law and Personal Information Protection Law, and related legislative practices in the United States, this article finds that current international data governance exhibits fragmentation, with significant differences among countries in data localization requirements, cross-border transfer conditions, and platform compliance obligations. The study proposes that the construction of a multilateral governance framework based on platform responsibility should adhere to the principle of "tiered governance": at the international legal level, unified data classification and cross-border flow standards should be established through a combination of soft and hard law; at the regional level, mutual recognition mechanisms and cooperation agreements should be promoted; and at the platform level, the "gatekeeper" responsibilities of transnational digital platforms should be strengthened, including obligations for data security, user rights protection, and regulatory cooperation. This article further demonstrates the necessity of a "dynamic balance" mechanism, which, while safeguarding national security and public interests, aims to standardize and facilitate cross-border data flows through tools such as adequacy determinations, standard contractual clauses, and binding corporate rules. The study argues that an international legal approach centered on platform responsibility can help bridge institutional differences across countries and provide a viable solution for building an inclusive, equitable, and sustainable global data governance system.

Keywords: data sovereignty, cross-border data flows, platform responsibility, multilateral governance, international data law.

Cite This Article:
Liao Peihong. (2025). Data Sovereignty And Cross-Border Data Flows Under The Multilateral Governance Framework: An International Legal Approach Based On Platform Responsibility. *International Journal of Advanced Research in Islamic Studies and Education (ARISE),* 5(4): 98-118.

INTRODUCTION

The advent of the digital economy has profoundly transformed the global governance landscape. As a new factor of production and strategic resource, the cross-border flow of data has become a key driver of international trade and technological innovation. Research by the United Nations Capital Development Fund Policy Accelerator (UNCDF Policy Accelerator, 2023) indicates that cross-border data flows increased 20-fold between 2007 and 2017, and are projected to increase another 4-fold between 2017 and 2022. Global data storage is projected to grow from 33 zettabytes in 2018 to 175 zettabytes in 2025, nearly half of which will be stored in the cloud. However, the unique properties of data present unprecedented challenges to its cross-border flow.

On the one hand, governments around the world have enacted restrictive data localization policies based on considerations such as national security, privacy protection, and economic sovereignty. Research by the Information Technology Innovation Foundation (Castro et al., 2021) shows that data localization measures have spread rapidly around the world, more than doubling from 67 measures in 35 countries in 2017 to 144 restrictive measures in 62 countries. Furthermore, research shows that using a data restrictiveness index based on OECD market regulation data, for every 1-point increase in a country's data restrictiveness, its total trade output decreases by 7%, productivity falls by 2.9%, and downstream prices rise by 1.5%.

On the other hand, the globalized digital economy requires the free and secure cross-border flow of data to optimize resource allocation and promote innovation. A McKinsey & Company (2022) study indicates that 75% of countries worldwide currently implement some degree of data localization rules, significantly impacting companies' IT infrastructure, data governance, and data architecture, as well as their interactions with local regulators.

Against this backdrop, the traditional international legal framework faces challenges in the digital age. A report by Chatham House (Afina et al., 2024) notes that countries differ significantly in their approaches to platform regulation, with no clearly established norms or best practices, and multilateral organizations failing to provide sufficient leadership at the international level. Major centers of digital power—Brussels, Beijing, London, and Washington—are pursuing distinctly different regulatory models.

COMPARISON OF THREE DATA GOVERNANCE MODELS

The EU, the US, and China, the world's three largest digital economies, have developed distinct models of data governance, a divergence that has been widely discussed in academic literature. Through the GDPR, the EU has established a strict regulatory system centered around personal data protection. Haagensen (2023) notes that this conflict is reflected in the varying enforcement mechanisms of national data protection laws, with some jurisdictions implementing strict measures while others adopt a more flexible approach. The EU considers personal data rights a fundamental right, as defined in the Charter of Fundamental Rights of the European Union, giving the EU data protection framework a non-economic objective.

The United States favors a market-oriented, light-touch regulatory model that emphasizes the free flow of data. A Chatham House study (Afina et al., 2024) shows that US regulation is characterized by a "light legal framework," minimizing government oversight of the internet and relying heavily on company self-regulation. The US maintains a hardline stance on the free flow of data, while restricting outflows based on national security. This nationalist stance, mixed with ideological factors, reflects the pursuit of maximizing US data interests.

China, on the other hand, has adopted a regulatory model focused on data security and national sovereignty. While China has long upheld data sovereignty, citing national data security as a pretext, it relaxed its ex ante regulatory efforts in 2024, emphasizing comprehensive oversight, including pre-, in-, and post-process oversight. This suggests that China is shifting toward more relaxed rules for cross-border medical data flows, advocating for a model of free information flow with strong economic incentives (Zhang et al., 2024).

THE RISE OF PLATFORM RESPONSIBILITY

In its "Guiding Principles on the Governance of Digital Platforms" (UNESCO, 2024), UNESCO emphasizes that digital platforms have become a new frontier for promoting peace, but also an ecosystem for misinformation, disinformation, ideological polarization, and incitement to violence. These principles clearly outline five overarching principles for digital platform governance: platforms' content curation and review policies and processes should be transparent; checks and balances should be formally institutionalized; governance processes should be open and accessible to all stakeholders, including the most vulnerable and marginalized groups; diverse expertise should be a common feature of all regulatory arrangements; and governance should protect and promote cultural diversity.

Chatham House (Afina et al., 2024), through a review of 55 laws and legislative proposals worldwide, identified five global trends in digital platform regulation: strict regulation, independent regulation, user rights and capabilities, extensive platform monitoring, and data localization as part of content moderation regulation.

To address this challenge, this study proposes an international legal approach centered on platform responsibility, aiming to reconcile the conflict between data sovereignty and cross-border data flows by building a multilateral governance framework. The core concept of this approach is to treat transnational digital platforms as the "gatekeepers" of data flows, assigning them corresponding legal responsibilities and obligations, while ensuring the effective fulfillment of these responsibilities through international cooperation mechanisms.

THEORETICAL BASIS AND REALISTIC CONFLICTS BETWEEN DATA SOVEREIGNTY AND CROSS-BORDER DATA FLOW

The Concept and Evolution of Data Sovereignty

Data sovereignty, as an extension of the traditional concept of sovereignty in the digital age, has its theoretical foundations traced back to the principle of sovereign equality established by the Treaty of Westphalia. However, the intangibility, reproducibility, and global mobility of data pose challenges to traditional sovereignty theories. Imperva (2023) defines data sovereignty as the concept that data is subject to the laws and governance rules of the country or region where it is collected, while data localization requires that the initial collection, processing, and storage of such data occur within the borders of that country.

The rise of the concept of data sovereignty is closely tied to the development of internet technology. The earliest data localization measures can be traced back to a 2005 law passed by the Kazakh government requiring all ".kz" domain names to be operated domestically (with later exceptions for Google and others). However, the push for data localization increased significantly following the 2013 revelations by Edward Snowden about US counterterrorism surveillance programs. Since then, governments around the world have expressed a desire to control the flow of citizens' data through technology (Wikipedia, 2024).

China has played a significant role in this development. Chen (2024) notes that China's stance and advocacy on data sovereignty are reflected in its Global Initiative on Data Security, which promotes data sovereignty by respecting the sovereignty, jurisdiction, and data security rights of all countries. The initiative states that countries should not require domestic companies to store data generated or obtained abroad within their own countries; countries should respect the sovereignty, jurisdiction, and data security management rights of other countries and should not directly obtain data located in other countries from companies or individuals without the legal permission of other countries. By March 2021, countries and regional organizations such as Russia, Pakistan, Cambodia, ASEAN, and the Arab League had clearly expressed their support for the Global Initiative on Data Security.

Economic Value and Technological Requirements of Cross-Border Data Flow

Cross-border data flows have become essential infrastructure for the modern digital economy. Research by the United Nations Capital Development Fund Policy Accelerator (UNCDF Policy Accelerator, 2023) indicates that data-driven services, such as computing, telecommunications, media, finance, and professional services, now account for half of cross-border trade in services, roughly equivalent to travel, transportation, and other traditional services combined. Video, gaming, and social sharing accounted for 80% of internet traffic in 2020.

Data may flow into, out of, or simply transit a country. Border crossings may be intentional (e.g., a Fijian resident sharing a file with a Bangladeshi resident) or unintentional (e.g., a Gambian resident sending an email to another Gambian resident, but the data is routed through a server in the United States). Intellectual property owners have broad discretion over the global distribution and use of their proprietary technology and content (UNCDF Policy Accelerator, 2023).

However, this data flow faces increasing restrictions. An OECD trade policy paper (Hinrich Foundation, 2023) shows an increase in the number of explicit data localization measures: by early 2023, there were 96 measures and four draft regulations in 40 countries; nearly half of these measures appeared after 2015; and these measures are becoming more stringent, with more than two-thirds involving storage requirements with movement bans by early 2023.

Fragmentation of the current governance model

Current global data governance is markedly fragmented. Research by the Center for International Governance Innovation (Kalkar & González Alarcón, 2023) notes that balancing individual privacy rights with the enormous potential of data sharing for innovation and the greater public good presents multifaceted challenges. Ongoing concerns surrounding data collection, storage, and utilization continue to raise ethical and legal dilemmas, complicating efforts to find a sustainable balance. This fragmentation is mainly reflected in the following aspects:

1. First, there are differences in legal frameworks. Vasylyk (2022)'s research indicates that the complexity of cross-border data governance regulations across countries is often described by international business scholars as a "complex" and "diverse" institutional environment. This disparity is particularly acute in the area of cloud service providers. Most EU companies, as well as national and EU organizations, rely on US cloud giants for data storage, with Amazon Web Services being a prime example.
2. Secondly, there are diverging regulatory approaches. Research by Chatham House (Afina et al., 2024) found significant differences between countries in their approaches to platform regulation, with no clearly established norms or best practices. Multilateral organizations are failing to provide sufficient leadership at the international level. Major centers of digital power are pursuing distinctly different regulatory models.
3. Finally, there is a lack of uniformity in enforcement mechanisms. The Global Data Governance Mapping Project (2021), which assessed data governance metrics across 68 countries and the European Union, found significant differences across countries across six attributes of data governance: strategy; laws and regulations; structural change; human rights and ethical standards; public participation; and international cooperation mechanisms.

COMPARATIVE ANALYSIS OF DATA GOVERNANCE LEGAL FRAMEWORKS IN MAJOR COUNTRIES AND REGIONS

EU GDPR Model: A Regulatory System Focused on Rights Protection

Through the GDPR, the EU has established the world's most stringent personal data protection system. This system, centered on the protection of individual rights, sets strict conditions and procedures for cross-border data transfers. Jones Day (2023) analyzed that Article 45 of the GDPR stipulates that data transfers covered by an adequacy decision can be carried out without the need for further legal safeguards (such as the European Commission's standard contractual clauses or binding corporate rules).

The cross-border data transfer mechanism under the GDPR framework mainly includes three paths: adequacy decision, appropriate safeguards, and exceptions in specific circumstances. Kiteworks (2025) detailed the applicable conditions of these mechanisms:

1. Adequacy Decision Mechanism : This is the most convenient data transfer tool provided by the GDPR. As of 2024, the European Commission has issued adequacy decisions for 15 countries and regions, including Andorra, Argentina, Canada (commercial organizations), the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, South Korea, Switzerland, the United Kingdom, the United States (commercial organizations participating in the European and American data privacy framework), and Uruguay (Iubenda, 2023).
2. Standard Contractual Clauses (SCCs) : For third countries without an adequacy decision, standard contractual clauses have become the most commonly used safeguard for data transfers. Hogan Lovells (2023) notes that on June 4, 2021, the European Commission adopted two sets of standard contractual clauses: SCCs governing the relationship between controllers and processors; and SCCs serving as a tool for data transfers outside the European Economic Area. These new SCCs were amended following the Schrems II ruling to address concerns about US intelligence collection activities.
3. Binding Corporate Rules (BCRs) : These are specialized mechanisms for data transfers within multinational corporations. Hogan Lovells (2023) suggests that BCRs are legally binding internal rules adopted by multinational corporations to facilitate the transfer of personal data to non-EEA countries in accordance with Articles 46(2)(b) and 47 of the GDPR. Compared to the European Commission's Standard Contractual Clauses (SCCs), BCRs are separately approved by European data protection authorities and therefore provide a higher level of legal certainty for companies transferring personal data across borders.

The Chinese Model: A Control System Focused on Data Security and National Sovereignty

China has established a data governance legal system centered on the Cybersecurity Law, the Data Security Law, and the Personal Information Protection Law, emphasizing data security and national sovereignty. However, in recent years, China has relaxed its restrictions on cross-border data transfers.

White & Case (2024) noted that on March 22, 2024, the Cyberspace Administration of China (CAC) released the much-anticipated final version of the "Regulations on Promoting and Regulating Cross-Border Data Flows," which took effect immediately. The regulations aim to reduce the burden of compliance requirements for cross-border data transfers and are considered part of China's efforts to stimulate economic growth and attract foreign investment.

Data Outbound Security Assessment Mechanism :

This is one of China's core mechanisms for cross-border data transfers. The Library of Congress (2024) notes that the 2022 Measures require mandatory CAC data security assessments for any "important data" or, in certain circumstances, personal information transferred out of China. The 2022 Measures broadly define "important data" as "any data that, if tampered with, damaged, leaked, or illegally acquired or used, could endanger national security, economic operations, social stability, or public health and safety."

Standard Contractual Mechanism:

The Standard Contractual Measures for the Export of Personal Information, which came into effect on February 22, 2023, provide an alternative route for non-critical information infrastructure operators to export data abroad. Analysis by Inside Privacy (2024) indicates that the regulations make significant changes to the volume-based thresholds applicable to non-CII entities, both compared to the existing rules and the draft released in September 2023.

Personal Information Protection Certification Mechanism:

This is the third data outbound transfer mechanism. Bird & Bird (2024) pointed out that on March 16, 2023, the National Information Security Standardization Technical Committee (TC260) issued the draft "Requirements for Certification of Cross-Border Transfers of Personal Information," which aims to elevate the legal effect of PI certification from a low-level technical guidance document to a non-mandatory national standard.

Important changes under the new regulations :

The 2024 new regulations introduce a number of important relaxations. White & Case (2024) summarize the main changes:

> Increase in the quantity threshold: Non-critical information infrastructure operators that transfer the personal information of fewer than 100,000 individuals (excluding sensitive personal information) to overseas recipients are exempt from the relevant requirements, and the threshold is increased from 10,000 individuals to 100,000 individuals.
> Contractual necessity exemption: The outbound transmission of personal information that is necessary for the execution and performance of a contract to which an individual is a party (including cross-border shopping, cross-border mail and delivery, cross-border remittances, cross-border payments, cross-border account opening, flight and hotel reservations, visa processing, and examination service contracts) is exempted.
> Human Resources Management Exemption: The outbound transfer of employee personal information necessary for the implementation of cross-border human resources management that complies with legally established internal labor rules is exempted.

The US Model: Market-Oriented Light Regulation and Sectoral Legislation

The US data governance model has distinct federal characteristics. The US lacks unified data protection legislation at the federal level, relying primarily on departmental and state-level legislation. Chatham House (Afina et al., 2024) notes that US regulation is characterized by a "light touch legal framework," minimizing government oversight of the internet and relying heavily on company self-regulation.

Departmental legislation at the federal level : At the federal level, the United States primarily regulates data protection through industry-specific laws, such as the Health Insurance Portability and Accountability Act (HIPAA) for medical data and the Gramm-Leach-Bliley Act (GLBA) for financial data. This departmental approach contrasts sharply with the EU's comprehensive regulation.

The rise of state-level legislation : In recent years, US states have enacted their own data protection laws. Chatham House (Afina et al., 2024) noted that in September 2023, California successfully passed AB 587, requiring social media companies to submit reports on content moderation and policy decisions to the state government by January 2024.

Changing stance on cross-border data flows : It is worth noting that the United States has undergone significant changes in its stance on international data flows. Freedom House (2025) noted that in 2023, the former U.S. Trade Representative changed the U.S. stance on cross-border data flows during negotiations on the World Trade Organization's Joint Statement on Electronic Commerce Initiative. This was a surprising reversal of the United States' long-standing policy of supporting the free flow of data across jurisdictions to promote digital trade.

Comparative Analysis and Enlightenment of the Three Models

A comparative analysis of the data governance models of the EU, China, and the United States reveals the following characteristics and trends:

Table 1: Comparison of data governance models in major economies

Feature Dimension	EU model	The Chinese model	American model
Legislative Concept	Protection of personal rights	National security and data sovereignty	Market freedom and innovation
Regulatory approach	Unified and comprehensive legislation	Hierarchical classification management	Departmental legislation
Cross-border transfer conditions	Adequacy decisions, SCCs, BCRs	Safety assessment, standard contracts, certification	Market orientation and department requirements
Enforcement Mechanism	Independent Data Protection Authority	Unified management by the Internet Information	Federal and state division of law

		Office	enforcement
Development Trends	Global influence spreads	Gradual opening and facilitation	Active state legislation

This divergent development pattern has led to fragmented global data governance. As Vasylyk (2022) notes, these differences are particularly acute in the cloud service provider sector. Given the aforementioned uncertainty regarding data transfers, recent developments suggest that companies are shifting toward data localization. For example, Oracle's EURA Cloud Service addresses growing customer demand for cloud services designed for, located in, and operated by EU personnel.

Construction of Platform Liability Theory and Application of International Law

The "gatekeeper" status of digital platforms is established

Digital platforms play a critical role as gatekeepers in global data flows, a position established both by technological realities and by legal imperatives. UNESCO (2024) explicitly states in its Guiding Principles on the Governance of Digital Platforms that the transformative role of digital platforms is undeniable. The same digital platforms that have advanced human rights, democratized access to knowledge and culture, and fostered global connections have also become ecosystems rife with misinformation, disinformation, ideological polarization, and incitement to violence.

Chatham House (Afina et al., 2024), through an in-depth analysis of 55 laws and legislative proposals worldwide, found that governments have undergone a significant shift over the past decade, from a reluctance to regulate to active guidance of digital platforms to address perceived harms and strengthen state oversight and control. Digital sovereignty is becoming a key goal of government policy, but this agenda is complicated by national security concerns, the influence of technology companies, and domestic politics.

From a technical perspective, digital platforms control the critical infrastructure for data flows. Research by the UNCDF Policy Accelerator (2023) shows that data generated by content or consumed by humans represents the majority of cross-border data volume. In 2020, video, gaming, and social sharing accounted for 80% of internet traffic. This means that a small number of large platforms effectively control the majority of global data flows.

From a legal perspective, the platform's "gatekeeper" status requires it to bear corresponding legal responsibilities. This responsibility is reflected not only in its technical capabilities, but also in its obligations to users, regulators, and the public interest.

Construction of a multi-level framework for platform responsibility

Based on existing international law theories and practices, this study proposes a multi-level framework of platform responsibility, which includes three levels: technical responsibility, legal responsibility, and social responsibility.

Technical responsibility level

Technical responsibilities primarily concern the obligations of platforms in terms of data security, privacy protection, and system reliability. The UNESCO (2024) Guiding Principles emphasize that platforms should commit to ensuring that their design processes, content moderation, and curation policies and practices are consistent with international human rights standards. This includes:

1. Data security obligations: Platforms should implement appropriate technical and organizational measures to protect data security and prevent data leakage, tampering or unauthorized access.
2. Privacy protection obligations: Platforms should design systems that comply with privacy protection principles and ensure the legality, fairness and transparency of data processing.
3. System reliability obligations: The platform should ensure the stability and reliability of its technical systems to avoid data loss or service interruption due to technical failures.

Legal responsibility level

Legal liability involves the compliance obligations and legal risks that platforms bear in different jurisdictions. Research by Chatham House (Afina et al., 2024) shows that platforms face multiple, sometimes conflicting, legal requirements from different jurisdictions.

ISACA (2024) case study mentions the challenge Microsoft faced in 2020 when the US government ordered it to provide access to data stored in its Irish data centers, despite Irish and EU laws protecting that data under the EU General Data Protection Regulation (GDPR). This case highlights the issue of conflicting jurisdictions and demonstrates the complexity of managing data sovereignty in a global cloud environment.

Social responsibility level

Social responsibility involves platforms' contributions to the public good and the prevention of potential social harm. UNESCO (2024) emphasizes that platforms should be able to manage and mitigate human rights risks associated with potentially harmful content, and should commit to ensuring that their design processes, content moderation, and curation policies and practices are consistent with international human rights standards and that they are transparent and accountable.

THE STATUS OF PLATFORM LIABILITY IN INTERNATIONAL LAW

The status of platform responsibility in international law is undergoing a significant shift from marginal to central. Traditional international law primarily regulates relations between states, with private entities generally considered objects rather than subjects of international law.

However, the rise of digital platforms and their crucial role in global governance have challenged this traditional understanding.

The development trend of international soft law

UNESCO's (2024) Guiding Principles on the Governance of Digital Platforms represent a significant international effort to standardize platform responsibility. While not binding, these principles provide an important reference for countries to formulate relevant laws and regulations. They clearly define the duties, responsibilities, and roles of states, digital platforms, intergovernmental organizations, civil society, the media, academia, the technical community, and other stakeholders, placing freedom of expression and access to information at the core of digital platform governance.

The 2024 Multilateralism Index, released by the International Peace Institute (IPI), shows that despite challenges, participation in the multilateral system has increased in virtually all areas except trade. This suggests that member states remain actively engaged in the system, even if the nature of that engagement has shifted from cooperation to competition.

Legal practice at the regional level

The European Union is at the forefront of legalizing platform liability. Chatham House (Afina et al., 2024) notes that an innovative regulatory package has emerged within the EU aimed at updating and rebalancing the intermediary liability protections provided by the EU's E-Commerce Act (2000). These initiatives include the 2018 Code of Conduct on Disinformation, the 2022 Regulation on Countering Terrorist Content Online, and the far-reaching Digital Services Act (DSA).

In Asia, the Japanese government has taken a proactive approach to addressing challenges facing companies, such as fragmented data regulations and data localization requirements. The Japan Times (2024) reported that during Japan's 2023 presidency, the G7 group endorsed the establishment of the Institutional Arrangements Partnership (IAP). Under the OECD framework, the IAP aims to promote international coordination to address issues related to cross-border data flows.

International trend of platform self-regulation

Research by Chatham House (Afina et al., 2024) found that during a 2018 hearing before the U.S. House of Representatives Commerce and Energy Committee, Mark Zuckerberg confirmed that the changes Facebook had made in response to the EU General Data Protection Regulation (GDPR) would be rolled out globally. However, the extent to which the European regulation has actually brought about change is controversial, as is the extent of the enforcement threat.

This "Brussels Effect" demonstrates that even in the absence of a unified global legal framework, regulatory policies of major economies can exert global influence through market forces. This provides important insights into the development of an international legal approach based on platform responsibility.

DESIGN OF A MULTILATERAL GOVERNANCE FRAMEWORK BASED ON PLATFORM RESPONSIBILITY

Theoretical Construction of the "Hierarchical Governance" Principle

Based on the above analysis, this study proposes the principle of "tiered governance" as the core concept for building a multilateral governance framework. This principle holds that effective global data governance requires a coordinated and unified governance system at the three levels of international law, regional cooperation, and platform self-regulation.

International law: a normative system combining soft law and hard law

At the international legal level, unified standards for data classification and cross-border flows should be established through a combination of soft and hard law. "International Data Governance: A Pathway for Progress," endorsed by the United Nations System Chief Executives Board (2023), provides an important reference for this aspect of governance. This document outlines a vision for international data governance, and its annexes serve as analytical resources to support member states' efforts.

The strength of soft law mechanisms lies in their flexibility and inclusiveness. While not legally binding, the UNESCO (2024) Guiding Principles provide important guidance for national policymaking by establishing common standards and best practices. Their five overarching principles—transparency, checks and balances, inclusiveness, diverse expertise, and the protection of cultural diversity—can serve as the foundation for international soft law norms.

Hard law mechanisms establish binding legal obligations through treaties and international agreements. Research by the Center for Global Development (2021) suggests that a global (or near-global) approach to data and data flow governance is needed to prevent further fragmentation, but there are disagreements on the best way forward, including a heated debate over whether initiatives to establish regional standards for cross-border data flows will foster or hinder greater global cooperation.

Regional cooperation level: mutual recognition mechanism and cooperation agreement

Regional cooperation is crucial for bridging global governance gaps. The G7 Institutional Arrangements Partnership (IAP), promoted by the Japanese government (2024), is a prime example of regional cooperation. The IAP is a mechanism that fosters multi-stakeholder, public-private, and cross-organizational collaboration to seek practical and effective solutions to data governance issues. Expected outcomes may include the development of guidelines, principles, reports, and technical cooperation, as well as recommendations for member countries to adhere to OECD recommendations.

Another important example of regional cooperation is the data flow cooperation mechanism in the Guangdong-Hong Kong-Macao Greater Bay Area. Bird & Bird (2024) pointed out that on June 29, 2023, the CAC and the Innovation, Technology and Industry

Bureau of the Hong Kong Special Administrative Region Government signed the "Memorandum of Understanding on Promoting Cross-Border Data Flows in the Guangdong-Hong Kong-Macao Greater Bay Area", aiming to establish a secure cross-border data flow mechanism for the Greater Bay Area under the national cross-border data transmission security management framework.

Platform self-discipline: Strengthening the responsibility of "gatekeepers"

At the platform level, the "gatekeeper" responsibilities of transnational digital platforms need to be strengthened. This responsibility includes three core elements:

1. Data security obligations : The platform should establish a comprehensive data security management system to ensure the security of data during collection, storage, transmission and processing.
2. User rights protection responsibility : The platform should protect users' data rights, including the right to know, the right to access, the right to correct, the right to delete, etc.
3. Regulatory cooperation obligations : The platform should actively cooperate with regulatory authorities in various countries, respond to regulatory requirements in a timely manner, and provide necessary technical support.

Construction of the "dynamic balance" mechanism

This study proposes a "dynamic balance" mechanism as a core tool to reconcile the conflict between data sovereignty and cross-border data flows. The core concept of this mechanism is to standardize and facilitate cross-border data flows through flexible institutional arrangements while safeguarding national security and public interests.

Internationalization of the adequacy recognition mechanism

The adequacy determination mechanism is the most convenient data transfer tool under the GDPR framework, and its international promotion is of great significance. Jones Day (2023) pointed out that the adequacy determination of the European and American data privacy frameworks applies to all data transfers to US companies under the GDPR, regardless of the transfer tool used. It will also facilitate transfers under the EU Standard Contractual Clauses (SCCs) and binding corporate rules.

However, the adequacy determination mechanism also faces challenges. Hogan Lovells (2023) notes that, given the invalidation of the aforementioned frameworks ("Safe Harbor" and "Privacy Shield"), there may still be some voices in the legal community expressing concerns about DPF. However, the European Commission's adequacy decision is binding, meaning that EU data protection authorities must accept it as a valid mechanism for establishing transatlantic data transfers compliant with Chapter V of the GDPR without obtaining any further authorization.

Table 2: Comparison of global data transmission protection mechanisms

Mechanism Type	Scope of application	Legal effect	Difficulty of implementation	flexibility
Determination of sufficiency	Recognized countries/regions	Highest	Low	Low
Standard Contractual Clauses	Globally applicable	medium	medium	medium
Binding Corporate Rules	Within the corporate group	high	high	high
Authentication mechanism	Specific industries/fields	medium	medium	medium

Standardization of standard contract clauses

Standard Contractual Clauses (SCCs), the most widely used data transfer safeguard, are crucial for reducing the fragmentation of global data governance. Analysis by Iubenda (2023) indicates that Standard Contractual Clauses (SCCs) are standardized clauses approved by the European Commission that allow for data transfers outside the European Economic Area (EEA). Both parties involved in a data transfer are required to sign an agreement containing the SCCs, without altering the text.

The UK has established its own standard contractual mechanism after Brexit. Technology Law Dispatch (2024) notes that on December 19, 2023, the Information Commissioner's Office (ICO) published updated guidance on the UK's Binding Corporate Rules (BCRs), introducing the UK BCR Appendix for Controllers and Processors (the Appendix). This will enable organizations with existing EU BCRs to include data transfers from the UK.

Global promotion of binding corporate rules

As the "gold standard" for data transfers within multinational corporations, the global adoption of binding corporate rules (BCRs) is crucial for promoting international investment and trade. Hogan Lovells (2023) notes that, amid the turmoil caused by the European Court of Justice's "Schrems II" ruling, BCRs are poised to maintain their reputation as the most powerful mechanism and the "gold standard" for the international transfer of personal data subject to the GDPR. Given recent and potential actions regarding the adequacy of European and American data privacy frameworks, BCRs may once again serve as a transfer mechanism that ensures long-term legal certainty.

Multi-stakeholder Participation Mechanism

An effective multilateral governance framework requires broad multi-stakeholder participation. The Digital Watch Observatory (2023) emphasizes that data governance in a multilateral environment requires the participation of multilateral organizations such as the G7, G20, the United Nations, and the OECD. These organizations have put forward various proposals related to data governance and its role in achieving the Sustainable Development Goals, particularly SDG 16 (peace, justice, and strong institutions) and SDG 17 (partnerships for the goals).

Intergovernmental cooperation mechanism

Intergovernmental cooperation is the foundation of multilateral governance. The UN System Chief Executives Board's (2023) document, "International Data Governance: A Pathway for Progress," emphasizes the important role of the UN system in promoting cooperation on international data governance. The document was developed by the High-Level Programme Committee (HLCP) Working Group on International Data Governance, co-chaired by the United Nations Office on Drugs and Crime (UNODC) and the World Health Organization (WHO), and comprised of members of the Committee of Statisticians of the United Nations System, policy staff, and data and digital technology experts.

Private sector engagement mechanism

The private sector, particularly digital platform companies, is a key player in data governance. Research by Chatham House (Afina et al., 2024) shows that platforms have significant discretion in how to manage government data access requests. For countries seeking to more closely regulate speech or behavior, US-based data storage hinders their attempts to identify offending users.

Civil society participation mechanism

Civil society organizations play a crucial oversight and advocacy role in data governance. A Freedom House (2025) report highlights that as more governments turn to data localization, the negative impact of these laws on digital rights is becoming increasingly apparent. The multi-stakeholder community must come together to develop rights-respecting solutions in response. The UNESCO (2024) Guiding Principles specifically emphasize the role of civil society: they are important watchdogs, monitoring, evaluating and reporting on laws, policies, regulatory actions, and the conduct of digital platforms that impact human rights. They should be required and able to manage and mitigate human rights risks associated with potentially harmful content.

CONCLUSION AND POLICY RECOMMENDATIONS

RESEARCH CONCLUSIONS

This study, through an in-depth analysis of the current state of global data governance, and in particular a comparative study of the three different governance models of the European Union, China, and the United States, draws the following key conclusions:

Data governance fragmentation is becoming increasingly serious

Global data governance is currently characterized by significant fragmentation, with significant differences between countries in data localization requirements, cross-border transfer conditions, and platform compliance obligations. According to ITIF (2021), data localization measures increased from 67 in 35 countries in 2017 to 144 in 62 countries. This policy divergence has severely impacted the development and efficiency of the global digital economy.

Platform responsibility becomes the focus of governance

Digital platforms are increasingly playing a prominent role as gatekeepers in global data flows, and platform responsibility has become a key focus of data governance policies across countries. UNESCO's (2024) guiding principles clarify the responsibilities of platforms in protecting freedom of expression and access to information, marking a significant shift in the international community's understanding of platform responsibility.

Multilateral cooperation mechanisms need to be improved urgently

The existing international legal framework is unable to effectively address the governance challenges of the digital age, and new multilateral cooperation mechanisms are needed. The document of the UN System Chief Executives Board (2023) provides an important framework for international data governance cooperation, but more specific implementation mechanisms and safeguards are still needed.

The "tiered governance" model is feasible

Through the coordination and collaboration of international law, regional cooperation, and platform self-regulation, a "tiered governance" model can effectively balance the contradiction between data sovereignty and cross-border data flows. The G7 IAP mechanism promoted by the Japanese government (2024) provides a useful exploration for the implementation of this model.

POLICY RECOMMENDATIONS

Based on the research conclusions, this paper puts forward the following policy recommendations:

Policy recommendations at the international level

Promote the formulation of soft law norms for international data governance. It is recommended that the development of global soft law norms for data governance be promoted within the UN framework, based on the UNESCO (2024) Guiding Principles on the Governance of Digital Platforms, to further improve international standards for data classification, cross-border transfer, and platform responsibility. Such norms should have the following characteristics:

1. Inclusive: encompassing countries at different levels of development and governance models.
2. Flexibility: Allowing countries to make appropriate adjustments based on their national conditions
3. Foresight: Consider emerging technologies and future trends

Establishing an international data governance dispute resolution mechanism

It is recommended to establish a dedicated data governance dispute resolution mechanism within the existing international legal framework to provide an effective solution for cross-border data flow disputes. This mechanism should include:

1. Early warning system: timely identification and prevention of potential disputes.
2. Mediation and Arbitration Procedures: Providing Diverse Dispute Resolution Options.
3. Implementation guarantee mechanism: ensuring the effective implementation of dispute settlement results.

Policy Recommendations At The Regional Level

Promote the construction of regional data governance coordination mechanism

It is recommended that regional organizations refer to the G7 IAP model promoted by the Japanese Government (2024) and establish a data governance coordination mechanism that suits the characteristics of their region. This mechanism should focus on:

1. Mutual recognition of systems: promoting mutual recognition of data protection systems in different countries
2. Standard unification: Develop regional unified data governance technical standards
3. Information sharing: Establish a regional data security information sharing platform

Promoting the free flow of data within the region

It is recommended that, on the premise of ensuring data security, unnecessary restrictions on data flow within the region should be gradually lifted, and reference should be made to the experience of the EU GDPR and China's Guangdong-Hong Kong-Macao Greater Bay Area cooperation mechanism to establish data flow facilitation arrangements suitable for the region.

Policy recommendations at the national level

Improve the domestic legal framework for data governance

It is recommended that countries improve their domestic legal frameworks for data governance based on their own national conditions and international best practices. In particular:

1. Clarify data classification standards: Establish a scientific and reasonable data classification system
2. Optimizing regulatory procedures: Improving the efficiency of data export approval
3. Strengthening law enforcement capabilities: Building a professional data governance law enforcement team.

Strengthening international cooperation and dialogue

It is recommended that governments actively participate in international data governance dialogue and cooperation, and promote the harmonization of data governance rules through bilateral and multilateral channels. China's Global Initiative for Cooperation on Cross-Border Data Flows, released in 2024, provides a useful reference for such cooperation.

Policy recommendations at the platform level

Establish a platform data governance and compliance system

It is recommended that digital platform companies establish a globally unified data governance and compliance system to ensure that compliance requirements in different jurisdictions are effectively met. This system should include:

1. Compliance management system: Establish a complete compliance organizational structure and process
2. Technical safeguards: Use advanced technology to ensure data security and privacy protection
3. Transparency Report: Regularly publish data governance transparency reports.

Strengthening multi-stakeholder engagement

It is recommended that platform companies actively participate in multi-stakeholder dialogues, establish long-term cooperative relationships with governments, civil society organizations and academic institutions, and jointly promote responsible data governance practices.

RESEARCH PROSPECTS

Although this study provides a theoretical basis and policy recommendations for a multilateral data governance framework based on platform responsibility, there are still some issues that need further research:

The impact of technological development

The development of emerging technologies such as artificial intelligence, blockchain, and quantum computing will have a profound impact on data governance, and further research is needed to examine the challenges and opportunities these technologies pose to existing governance frameworks.

Special needs of developing countries

Developing countries face special challenges in data governance capacity building, technical infrastructure, and talent training, and need to specifically study data governance paths suitable for developing countries.

The role of emerging governance entities

In addition to traditional governments and enterprises, the role of emerging governance entities such as technology communities, standardization organizations, and third-party auditing agencies is becoming increasingly important, and further research is needed on the positioning and role mechanisms of these entities in the multilateral governance framework.

In general, building a multilateral data governance framework based on platform responsibility is a complex systematic project that requires the concerted efforts and ongoing exploration of the international community. This study provides theoretical support and practical guidance for this endeavor, and we look forward to further refinement and development in future research and practice.

REFERENCES

Afina, M., McDonald, S., & McQuinn, A. 2024. Towards a global approach to digital platform regulation. Chatham House. https://www.chathamhouse.org/2024/01/towards-global-approach-digital-platform-regulation.

Bird & Bird. 2024. China data protection and cybersecurity: Annual review of 2023 and outlook for 2024 (I). Bird & Bird Insights. https://www.twobirds.com/en/insights/2024/china/china-data-protection-and-cybersecurity-annual-review-of-2023-and-outlook-for-2024-1.

Castro, D., McLaughlin, M., & Chivot, E. 2021. How barriers to cross-border data flows are spreading globally, what they cost, and how to address them. Information Technology and Innovation Foundation. https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/.

Center for Global Development. 2021. How can multilateral organizations strengthen global data governance practices? Roundtable summary. https://www.cgdev.org/publication/how-can-multilateral-organizations-strengthen-global-data-governance-practices

Chen, J. 2022. Governing cross-border data flows: International trade agreements and their limits. *Laws*, 11(4), 63. https://doi.org/10.3390/laws11040063

Digital Watch Observatory. 2023. The challenges of data governance in a multilateral world. https://dig.watch/event/internet-governance-forum-2023/the-challenges-of-data-governance-in-a-multilateral-world.

Freedom House. 2025. Data localization: A global threat to human rights online. https://freedomhouse.org/article/data-localization-global-threat-human-rights-online

Global Data Governance Mapping Project. 2021. The global data governance mapping project. https://globaldatagovernancemapping.org/

Hinrich Foundation. 2023. The nature, evolution, and potential implications of data localization measures. https://www.hinrichfoundation.com/research/how-to-use-it/the-nature-evolution-and-potential-implications-of-data-localization-measures/

Hogan Lovells. 2023. EU-U.S. data privacy framework: European commission takes third bite at the adequacy cherry. https://www.hoganlovells.com/en/publications/eu-us-data-privacy-framework-european-commission-takes-third-bite-at-the-adequacy-cherry_1

Imperva. 2023. What is data localization: Pros & cons. https://www.imperva.com/learn/data-security/data-localization/

Inside Privacy. 2024. China eases restrictions on cross-border data flows. https://www.insideprivacy.com/uncategorized/china-eases-restrictions-on-cross-border-data-flows/

International Peace Institute. 2024. Multilateralism index 2024. https://www.ipinst.org/2024/10/multilateralism-index-2024

ISACA. 2024. Cloud data sovereignty governance and risk implications of cross-border cloud storage. https://www.isaca.org/resources/news-and-trends/industry-news/2024/cloud-data-sovereignty-governance-and-risk-implications-of-cross-border-cloud-storage

Iubenda. 2023. Standard contractual clauses (SCCs), a complete guide. https://www.iubenda.com/en/help/107560-standard-contractual-clauses

Jones Day. 2023. EU and U.S. reach new agreement on data sharing. https://www.jonesday.com/en/insights/2023/07/eu-and-us-reach-new-agreement-on-data-sharing

Kalkar, U., & González Alarcón, N. 2023. The global landscape of data governance. Centre for International Governance Innovation. https://www.cigionline.org/articles/the-global-landscape-of-data-governance/

Kiteworks. 2025. Standard contractual clauses (SCCs): Benefits, requirements & limitations. https://www.kiteworks.com/risk-compliance-glossary/standard-contractual-clauses-sccs/

Library of Congress. 2024. China: New rules on cross-border data transfers released. https://www.loc.gov/item/global-legal-monitor/2024-05-13/china-new-rules-on-cross-border-data-transfers-released/

McKinsey & Company. 2022. Localization of data privacy regulations creates competitive opportunities. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/localization-of-data-privacy-regulations-creates-competitive-opportunities

Technology Law Dispatch. 2024. Introduction of a UK BCR addendum. https://www.technologylawdispatch.com/2024/02/regulatory/introduction-of-a-uk-bcr-addendum/

The Japan Times. 2024. International cooperation necessary to address data governance. https://www.japantimes.co.jp/2024/05/02/special-supplements/international-cooperation-necessary-address-data-governance/

UNCDF Policy Accelerator. 2023) . The role of cross-border data flows in the digital economy. https://policyaccelerator.uncdf.org/all/brief-cross-border-data-flows

UNESCO. 2024. Guidelines for the governance of digital platforms. https://www.unesco.org/en/internet-trust/guidelines

UN System Chief Executives Board for Coordination. 2023. International data governance – Pathways to progress. https://unsceb.org/international-data-governance-pathways-progress

Vasylyk, T. 2022. Unravelling cross-country regulatory intricacies of data governance: The relevance of legal insights for digitalization and international business. *Journal of International Business Policy*. https://link.springer.com/article/10.1057/s42214-023-00172-1

White & Case. 2024. China released new regulations to ease requirements for outbound cross-border data transfers. https://www.whitecase.com/insight-alert/china-released-new-regulations-ease-requirements-outbound-cross-border-data-transfers

Wikipedia. 2024. Data localization. https://en.wikipedia.org/wiki/Data_localization

Zhang, L., et al. 2024. Paradigm transformation of global health data regulation: Challenges in governance and human rights protection of cross-border data flows. PMC. https://pmc.ncbi.nlm.nih.gov/articles/PMC11668341/