Advances in Social Behavior Research Vol.16 Issue 5 EWA Publishing
Available Online: 25 July 2025 DOI: 10.54254/2753-7102/2025.25597

Research on the legal regulation of cross-border data flows in the context of the digital economy: start with the "Trilemma Theory"

Jingyi Wu

School of International Law, China University of Political Science and Law, Beijing, China

alyssakerr@163.com

Abstract. Against the backdrop of globalization's deepening evolution, the profound coupling between cross-border data flows and digital economic development is reshaping the global economic landscape. This dual-edged effect concurrently poses multidimensional risks to national data sovereignty, societal public security, and individual citizens' rights. Confronted with governing cross-border data flows, nations face the predicament of being unable to simultaneously achieve data protection sovereignty, unrestricted cross-border data flow, and data protection. Based on this, this article employs the "Trilemma Theory" to systematically deconstruct current global governance variations. It then analyzes the two predominant paradigms formed by the European Union and the United States, revealing their internal logic and oriented goals. Concurrently, it examines the current status and challenges of China's cross-border data flow regulation, aiming to explore a governance pathway suited to China. The goal is to build a governance ecosystem that balances high-level data openness with data security protection, serving both the digital economy's high-quality development and the safeguarding of national and public core interests.

Keywords: cross-border data flow, digital economy, Trilemma Theory, data security, data protection

1. Introduction

In the digital economy era, cutting-edge technologies such as artificial intelligence, blockchain, and cloud computing are evolving at an unprecedented pace, enabling diverse application scenarios. This deep integration between the digital and real economies is driving a transformation toward ubiquitous digitization. Data, without a doubt, has become a new key engine for economic growth in the digital age [1]. At its core, data serves as the carrier of information and symbols. When it undergoes multiple stage such as production, collection, storage, analysis, and circulation, and deeply integrates into the operation of the real economy, its value as a new production factor can be fully unleashed. With this, it empowers economic high-quality development through powerful productivity. Currently, the world economy is accelerating from a traditional model centered on the circulation of goods and capital to one dominated by the free flow of data and information [2]. Data cross-border flow is an inevitable requirement for the development and maintenance of the economic globalization process. Focusing on China, the scale of the digital economy reached 50.2 trillion yuan in 2022, with a nominal growth of 10.3% year-on-year. It has consistently outpaced the nominal growth rate of Gross Domestic Product (GDP) for 11 consecutive years. In 2023, the core industries of the digital economy in China generated an added value of over 12 trillion-yuan, accounting for 10% of the GDP. At the same time, "digital economy" and "accelerating the construction of Digital China" were mentioned multiple times in the government work report for 2025. Thus, the importance of cross-border data flow in the development of the digital economy has become increasingly prominent.

However, at present, China's digital economy development is mainly confronted with several key challenges, such as the relatively lagging construction of the data element market, the urgent need to improve the regulatory framework for platform economy, and the increasingly prominent risks of data security. Meanwhile, China's voice in the global digital economy governance system is relatively weak, which does not match the significant growth of its digital economy development. This incompatibility limits China's leading role in promoting the transformation of global digital economy governance. Therefore, enhancing the governance efficiency of data elements and accelerating the forging of new productive forces have become the strategic support for China to deepen high-level opening-up.

In this context, this article takes the governance of cross-border data flow as the main research object, and starts from the "Trilemma Theory" to explore the possible scenarios of cross-border data flow regulation. Then, it reviews and analyzes the achievements and problems of China in the governance of cross-border data flow. Meanwhile, from a comparative law

perspective, explores the advanced experiences of the European Union (EU) and the United States (US) in cross-border data flow, with the aim of providing new perspectives and ideas for China to improve its cross-border data flow governance. Finally, it attempts to put forward corresponding improvement suggestions to construct a governance path applicable to China.

2. Cross-border data flow and the Trilemma Theory

2.1. Mechanism of cross-border data flow

Organisation for Economic Co-operation and Development (OECD) refers to cross-border data as "the transmission of personal data across national borders" [3]. Subsequently, this definition has been influenced by a series of complex factors such as national strategic security, economic development level, and personal privacy protection, and has been continuously expanding worldwide but has not yet been unified [4]. At its core, this mainly encompasses two elements. On one hand, data refers to identifiable and readable data that contains specific information; on the other hand, the flow of data crosses national borders.

As the strategic value of data resources continues to increase, the concept of "cross-border data" is undergoing an expansion of its connotation and a reconfiguration of its scope. On one hand, the scope of data has expanded from the initially focused on personal data to cover data in multiple fields such as society, politics, and economy; on the other hand, its flow form is no longer limited to traditional active transmission and transfer, but also involves new interaction modes such as remote access, real-time retrieval, and cross-border utilization through the Internet based on the inherent non-physical attributes of data [5]. Specifically, cross-border data flow mainly includes two situations: the cross-border transmission and transfer of data, and even if the data is not cross-border, it can still be accessed and processed by foreign entities.

2.2. The significance of regulating cross-border data flow

Firstly, since the flow of data crosses national borders, it involves the interests of more than one country, including security issues. Due to the weak protection of critical information infrastructure and insufficient cybersecurity capabilities in many developing countries, if the free flow of cross-border data is allowed, their critical facilities will be easily targeted by attacks, thereby endangering the security of various fields such as politics, economy, and military of the country [6].

Secondly, from the perspective of industry development, some countries or regions have a leading position in the development of the data industry and the application of big data technology. Their digital infrastructure is relatively advanced. The free flow of cross-border data will create higher economic value for them [7]. In contrast, countries or regions with relatively weak digital technologies and related infrastructure will be impacted by the development of the digital industry, and thus generally hold a more conservative stance towards the free flow of cross-border data. Under this mechanism, data elements and resources will instead flow to those countries that are at the leading position, exacerbating the digital divide [8].

Furthermore, the cross-border flow of data may cause an impact on privacy protection. Therefore, safeguarding the data rights enjoyed by citizens is also one of the initial intentions of most countries in managing the cross-border data flow, and using laws and regulations to reduce the risk of illegal collection of personal information [9]. For example, in the context of human rights protection, the EU weighs the relationship between privacy protection and data flow through the principle of proportionality, even if data flow can bring economic benefits, it cannot be at the cost of sacrificing dignity, privacy, and basic restrictions on data protection [10].

2.3. The significance of regulating cross-border data flow

2.3.1. The Trilemma Theory

The Trilemma Theory originated from the Mundell-Fleming model and was initially introduced in the field of international economics. It is a term used in economic decision-making. The traditional Trilemma Theory states that an open economy cannot simultaneously possess a fixed exchange rate, an independent monetary policy, and free capital flows; it can only achieve two of the three policy goals [11]. For example, the Bretton Woods system is an example of choosing a fixed exchange rate system and ensuring free capital flows. This means that this system requires countries to give up monetary policy independence. Moreover, to maintain monetary policy independence and free capital flows, one needs to give up exchange rate stability and adopt a floating exchange rate; pursuing monetary policy autonomy and exchange rate stability will limit the complete flow of capital. Now, some scholars have also applied the Trilemma Theory to other fields. For instance, in the blockchain, the "Trilemma Theory" refers to the difficulty of simultaneously achieving security, decentralization, and scalability in the design of the blockchain system [12]. This article attempts to introduce the "Trilemma Theory" into cross-border data flow regulation, in order to explore the current regulatory models and future regulatory paths regarding this issue.

2.3.2. The Trilemma Theory in cross-border data flow regulation

In the context of cross-border data flow, the goals pursued by different countries are different. The autonomy of data protection, the free cross-border flow of data, and data protection constitute three mutually exclusive goals that cannot be achieved simultaneously [13]. Among them, data protection autonomy represents the power of sovereign states to independently manage data within their territory, with the core objective being to strengthen the country's control over data through measures such as data localization. Data protection focuses on privacy security, aiming to prevent data leakage. And the free flow of data emphasizes the ability for information to cross different jurisdictions, enabling unobstructed circulation of collection, transmission, and processing. In actual regulation, due to the difficulty of achieving these three goals simultaneously, countries often find themselves in a trilemma dilemma when choosing the governance model for cross-border data flow. Specifically, there are the following three scenarios:

Scenario 1: If various countries have full data autonomy and actively promote the free flow of cross-border data, they may inevitably relieve data regulation, resulting in poor protection of data. In this context, each country has the autonomy to formulate and implement its own data protection laws. When data flows across borders, conflicts regarding the application of data laws may arise. In such cases, in order to balance the data protection autonomy and the practical needs of cross-border data flow, during the rule coordination process, the level of data protection often needs to be lowered. Although this policy can effectively attract cross-border data inflows to a certain extent, due to the weakened data protection and inadequate data security measures, it is prone to data leakage or abuse, thus posing a significant threat to personal privacy and information security.

Scenario 2: If governments have full autonomy in data protection while also being committed to data protection, they are likely to adopt stricter data protection laws, which will pose obstacles to the cross-border flow of data. Such strict data protection systems, while strengthening citizens' privacy rights and national data security, objectively restrict the cross-border mobility of data. Specifically, first, such systems often mandate that data be stored and processed domestically and set strict compliance thresholds for data exports; second, significant differences in data protection legislation frameworks, regulatory systems, and enforcement effectiveness among different jurisdictions make the legal and compliance environment for cross-border data flow increasingly complex.

Scenario 3: To maintain the need for effective data protection and the free flow of cross-border data, it implies the loss of data protection autonomy. At this point, governments of various countries need to consider transferring some data protection sovereignty to supranational entities, or formulating unified and binding regulations through agreements.

Based on the aforementioned model, two predominant governance paradigms have emerged in global practice: the free flow model championed by the United States and the data protection model spearheaded by the European Union. The EU has established data protection sovereignty through comprehensive legislation, prioritizing the safeguarding of personal privacy. However, this approach imposes stringent restrictions on data transfers from the EU to external jurisdictions. Conversely, the US has forged its data protection sovereignty primarily through industry self-regulation mechanisms, advocating vigorously for the free flow of data across borders. Yet, this model is characterized by a relatively underdeveloped level of domestic data protection. These two models, with their differently prioritized objectives, epitomize the fundamental tension and debate between "data protection" and "unrestricted cross-border data flow." This divergence has profoundly shaped the evolution of the global governance framework for cross-border data flows. Crucially, governing cross-border data flows necessitates both domestic policy formulation and international rule coordination. The inherent variations in national legal regulations stem from differing policy orientations. The Trilemma Theory underscores the intrinsic tension and natural trade-offs among the core policy objectives pursued by nations, implying that achieving full realization of data protection sovereignty, unfettered cross-border data flow, and data protection simultaneously is inherently challenging; gains in one area often entail compromises in another.

3. Extraterritorial practices in cross-border data flow regulation

3.1. The free flow model

Certain nations have established governance frameworks prioritizing the free flow of data, with the objectives of facilitating unrestricted cross-border data flows, maintaining their leadership position within the digital economy, and advancing their economic and national interests. As the preeminent global technological power and a principal driver of the digital economy, the United States exemplifies this approach, being a leading proponent of the free flow governance model.

Firstly, the United States has not established unified domestic regulations for cross-border data flows. Relevant legal provisions are fragmented across sectoral legislation, such as healthcare and education. Instead, it relies on an industry self-regulation model for data protection [14]. The U.S. approach advocates situating personal data governance within a market-based framework, proposing that industry self-regulation establish norms for cross-border data flows. This model adheres to market-based regulatory principles, emphasizing the economic benefits and digital economy development fostered by unimpeded data movement [15]. Consequently, in governing cross-border data flows, the U.S. prioritizes free circulation as its core objective,

with economic interests and free trade serving as key policy drivers. It implements an industry self-regulation mechanism alongside stringent controls on data exports from critical sectors. Secondly, the United States strategically focuses on constructing multilateral data flow networks to facilitate overseas data acquisition. Internationally, in 2000, the U.S. negotiated the U.S.-EU Safe Harbor Framework to address EU data protection requirements, though it was invalidated in 2015. Subsequently, the EU-U.S. Privacy Shield was adopted in 2016. Under this mechanism, U.S. enterprises can establish compliance frameworks by voluntarily adhering to EU data protection standards to legally process EU personal data. However, this arrangement incorporates essential constraints: U.S. government or law enforcement access to relevant data must strictly follow predefined safeguards and legal procedures. Since 2005, the U.S. has promoted and implemented the Asia-Pacific Economic Cooperation (APEC) Privacy Framework, urging member economies to minimize unnecessary barriers to data flow to advance e-commerce [16]. Furthermore, the U.S. has incorporated its cross-border data flow principles into multiple agreements, including the Cross-Border Privacy Rules (CBPR), the Trans-Pacific Partnership (TPP), and its successor, the United States-Mexico-Canada Agreement (USMCA). These agreements reduce limitations on data storage and processing location and, notably in the USMCA, explicitly restrict data localization mandates.

Furthermore, the United States impose strict controls on data exports. Grounded in territoriality principles, the U.S. restricts the outflow of domestic data and technology while utilizing long-arm jurisdiction to facilitate the acquisition of foreign data [17]. The Clarifying Lawful Overseas Use of Data Act (CLOUD Act) of 2018 established the “data controller” standard. In disputes concerning foreign data acquisition and international jurisdiction, it significantly strengthened principles of personal jurisdiction, asserting U.S. government authority to access data stored abroad [18]. Specifically, regardless of the data’s physical location, if it is controlled by a U.S. person or entity, communication service providers must disclose it to U.S. authorities. This enables the U.S. government to extend its data jurisdiction extraterritorially based on the nexus of U.S. enterprise data service providers. Legal scholars observe that this Act allows the U.S. to transcend traditional territorial and personal jurisdiction principles in data governance, exhibiting clear extraterritorial application [19].

It can be concluded that the U.S. free flow governance model operates across domestic and international dimensions. Externally, it constructs mechanisms to facilitate the global inflow of data. Internally, it progressively tightens restrictions on the outward transmission of domestic data through rigorous regulatory policies.

3.2. The data protection model

The European Union maintains a sustained focus on the core imperatives of the digital economy, systematically constructing comprehensive governance frameworks. Notably, it regulates market order through forward-looking data regulatory systems and actively promotes the development of Common European Data Spaces to eliminate data silos among member states, industries, and sectors. Through its distinctive data policies, the EU has established the dual objectives of safeguarding fundamental rights and fostering a robust internal market [20]. This governance paradigm, initiated by the EU’s comprehensive legislative initiatives, has effectively shaped a globally influential model. Consequently, the EU successfully promulgates its standards within global cross-border data governance frameworks, thereby significantly bolstering its regulatory influence and discourse power in this critical domain.

Firstly, the EU has been actively establishing a comprehensive legal framework for data management. This framework is now principally underpinned by the General Data Protection Regulation (hereinafter “GDPR”), the Data Governance Act (hereinafter “DGA”), and the Data Act. Originating from its emphasis on personal data and privacy rights, the EU constructed a modern governance paradigm through the GDPR. This regulation expanded the definition of personal data to enhance protection coverage, established stringent informed consent standards to consolidate data subject rights, implemented a hierarchical accountability framework for data controllers and processors, and concurrently established enforcement mechanism among the members. This mechanism increases violation costs and guides enterprises towards legal compliance [21]. In 2022, the DGA further instituted a mechanism for the reuse of public sector data. This facilitates the provision of data by citizens and enterprises, promotes cross-sectoral and cross-border data utilization, fosters the establishment of a high-quality circulation system for diverse data types (including health, environment, agriculture, and public administration data), and reduces societal operational costs [22]. In 2024, the Data Act further supplemented aspects such as conditions for data utilization within this evolving framework.

At the same time, to elevate the level of data supervision, the EU has established two independent institutions: the European Data Protection Supervisor (EDPS) and the European Data Protection Board (EDPB). These bodies enhance the scientific basis of data governance decisions, safeguard data security, and promote the fair and orderly development of the EU’s digital economy market. Among these institutions, the EDPS’s core functions encompass supervising the end-to-end compliance of EU institutions with personal data processing rules, systematically assessing the potential impact of emerging technologies on the data protection framework, and providing corresponding recommendations for EU policymaking and legislation concerning personal data processing. The EDPB focuses on three key dimensions: exercising independent regulatory authority over digital platforms to ensure personal information security; formulating strategic policy recommendations for EU legislators; and conducting predictive monitoring and investigations into cutting-edge technologies posing potential risks to citizens’ privacy

rights. This structure forms a comprehensive governance loop covering policymaking, technology governance, and enforcement supervision.

Secondly, the EU has also intensified platform supervision to address the escalating monopolistic tendencies within digital platforms. Through the Digital Services Act (hereinafter "DSA") and the Digital Markets Act (hereinafter "DMA"), it aims to create a secure digital space and a fair business environment. The DSA establishes clear accountability systems for social media, online platforms, and intermediary service providers, achieving platform accountability by strengthening the governance of illegal online content and safeguarding fundamental user rights. Meanwhile, the DMA sets precise standards and boundaries for the conduct of designated "gatekeeper" platforms and service providers, replacing reliance on industry self-regulation with robust enforcement and punitive measures. This approach curbs the anti-competitive practices of large online platforms and protects consumer interests.

In conclusion, the EU promotes the formation of an internal data sharing mechanism through legislative and regulatory measures. The governance model it has established not only facilitates the free flow of data within the EU but also reinforces data protection, ensuring data security and controllability.

4. The impact on cross-border data regulations in China

4.1. The current situation and problems of cross-border data regulation in China

In the field of cross-border data flow regulation, China has established a legal framework comprising three foundational laws—Cybersecurity Law, Data Security Law, and Personal Information Protection Law—as the top-level structure, supplemented by implementing rules such as the Measures for Security Assessment of Data Exports, the Measures for Standard Contracts for Personal Information Exports, and the Provisions on Promoting and Regulating Cross-Border Data Flows. This framework prioritizes core policy objectives including safeguarding national data sovereignty, protecting personal information rights, and ensuring critical data security [23]. By defining localized data obligations, establishing security assessment systems, clarifying liability and supervisory entities, and implementing supporting regulations, it achieves refined controls over data exports, ultimately establishing a hierarchical governance system covering key aspects.

However, China's current regulation of cross-border data flows still faces several issues. The existing legislation primarily adopts a fragmented approach, lacking systematic coordination and comprehensive legislative design [24]. Simultaneously, the content of effective regulations consists mainly of general guidelines or principle-based provisions, exhibiting problems such as insufficient implementation details and an incomplete security assessment system. This relatively disjointed legislative framework and ambiguous legal provisions hinder the effective governance of cross-border data flows.

Furthermore, China's extraterritorial regulation of cross-border data flows remains limited [25]. Reviewing current legislation in this field, most provisions focus on domestic governance with inadequate consideration for extraterritorial jurisdiction. Given that asserting jurisdiction over data governance is a global trend, China still needs to strengthen its extraterritorial regulatory efforts compared to the US and the EU.

4.2. The construction and improvement of China's cross-border data regulation structure

In response to the aforementioned issues, China should carry out optimization in three dimensions and explore new paths for regulating cross-border data flows.

Firstly, it is necessary to enhance the legislation governing cross-border data flows to improve its operational effectiveness. China urgently needs to expedite the development of a top-level institutional framework for its data sovereignty strategy, with core objectives of enhancing the competitiveness of China's digital industry and strengthening the governance efficiency of government data. Ultimately, this should lead to the formation of a data sovereignty governance system and practice model with Chinese characteristics. Additionally, efforts should be made to refine the applicable standards within existing regulations. On one hand, the data classification and grading system established under Article 21 of the Data Security Law of the People's Republic of China should be fully implemented, clearly defining key concepts and delineating their scope [26]. Different exit pathways and protective measures could be adopted for different types and levels of data based on their importance. On the other hand, the assessment criteria for data exit should be enhanced, rationally delineating the focus of assessment and review, and providing clear, reasonable guidance for enterprises regarding data exit procedures [27]. Concurrently, the extraterritorial regulatory strength of data legislation should be appropriately reinforced. When formulating data legislation, attention must be paid to establishing the extraterritorial effect of jurisdictional clauses. This provides a legal basis for Chinese law enforcement and judicial institutions to exercise data governance rights across borders, thereby comprehensively safeguarding China's data interests.

Secondly, in-depth international cooperation should be pursued, and active participation in the formulation of international rules should be sought. Currently, no unified global regulation on cross-border data flows exists. China needs to enhance its

foresight and strategic thinking regarding global cross-border data flow rules, aiming to lead the construction of international institutional frameworks to promote the Chinese approach, and ultimately establish China's discourse power in shaping global cross-border data governance rules [28]. Currently, China has signed the Regional Comprehensive Economic Partnership Agreement (RCEP) and is actively preparing to join the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the Digital Economy Partnership Agreement (DEPA). Building on this, it can negotiate rules conducive to the development of China's digital economy. Adhering to the global governance principle of "extensive consultation, joint contribution, and shared benefits" and the principle of multilateral participation to seek consensus, China should explore leveraging the "Belt and Road Initiative" to conduct cooperation on cross-border data flow governance and supervision with participating countries.

Finally, it is necessary to flexibly respond to the evolving global digital economy environment and construct a new governance paradigm. As a new engine of global economic development, the digital economy is profoundly reshaping the international competitive landscape [29]. However, the current global digital economy governance system remains imperfect and is undergoing profound transformation. Against this backdrop, China urgently needs to balance development and security, focusing on building robust digital economy security barriers. Efforts should be made to strengthen security foundations and establish a security risk prevention and control system oriented towards development needs. By clarifying the three dimensions of overarching goals, key tasks, and guarantee mechanisms, China can comprehensively enhance its data security safeguard capacity, create a favorable environment for digital economy development, and promote the development of new quality productive forces.

5. Conclusion

With the deepening advancement of the new technological revolution and globalization, the networked open innovation paradigm has become increasingly prominent. Its advocated concept of openness and sharing aligns closely with the inherent mobility of data, effectively driving the free flow of global data. However, while cross-border data flow empowers digital economic development, it simultaneously poses multi-layered security challenges to national sovereignty, social stability, and citizens' rights. The core contradiction within the governance system lies in the Trilemma dilemma, where data protection sovereignty, unrestricted cross-border data flow, and data protection cannot be simultaneously achieved. Currently, cross-border data flow governance presents two predominant models: the data protection model championed by the European Union and the data free flow model emphasized by the United States. Based on this, China urgently needs to clearly define its strategic positioning in global digital governance: guided by the overall national security perspective, to promote a policy transformation prioritizing both development and security. On this foundation, it can seek to transcend traditional regulatory frameworks, enhance top-level legal design, and leverage new technologies to ensure the security of cross-border data flows. Concurrently, it is imperative to strike a balance between development and security, actively participate in bilateral and multilateral rule negotiations, and promote the establishment of a fair and orderly new order for cross-border data governance. This will strengthen China's discourse power in global digital governance and inject Chinese momentum into sustainable digital prosperity.

References

[1] Kowalkiewicz, M., Safrudin, N., & Schulze, B. (2017). The business consequences of a digitally transformed economy. *Shaping the Digital Enterprise: Trends and Use Cases in Digital Innovation and Transformation*, 29–67.

[2] Drucker, P. F. (1992). The new society of organizations. *Harvard Business Review*, *70*(5), 95–104.

[3] OECD. (1980). *OECD guidelines on the protection of privacy and transborder flows of personal data*. https: //www.oecd.org/digital/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[4] Kuner, C. (2013). *Transborder data flows and data privacy law*. Oxford University Press.

[5] Zhang, M. (2020). Cross-border Data Flow: Global Situation and the Countermeasures for China. *China Opening Journal*, (2), 44-50.

[6] Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers & Security, 120,* 102820.

[7] Meltzer, J. P. (2015). The Internet, Cross-Border Data Flows and International Trade. *Asia & the Pacific Policy Studies*, *2*(1), 90–102.

[8] Aaronson, S. A., & Leblond, P. (2018). Another digital divide: The rise of data realms and its implications for the WTO. *Journal of International Economic Law*, *21*(2), 245–272.

[9] Kuner, C. (2009). An international legal framework for data protection: Issues and prospects. *Computer Law & Security Review*, *25*(4), 307–317.

[10] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40–81.

[11] Obstfeld, M., Shambaugh, J. C., & Taylor, A. M. (2005). The Trilemma in History: Tradeoffs Among Exchange Rates, Monetary Policies, and Capital Mobility. *The Review of Economics and Statistics*, *87*(3), 423–438. https: //doi.org/10.1162/0034653054638300

[12] Quattrocchi, G., Scaramuzza, F., & Tamburri, D. A. (2024). The Blockchain Trilemma: An Evaluation Framework. *IEEE Software*, *41*(6), 101–110.
[13] Zheng, G. (2021). Trilemma and tripartition: The regulatory paradigms of cross-border personal data transfer in the EU, the US and China. *Computer Law & Security Review*, *43*, 105610.
[14] Listokin, S. (2015). Industry self-regulation of consumer data privacy and security. *J. Marshall J. Info. Tech. & Privacy L.*, *32*, 15.
[15] Shukla, S., Bisht, K., Tiwari, K., & Bashir, S. (2023). Comparative study of the global data economy. In *Data economy in the digital age* (pp. 63–86). Springer.
[16] Asia-Pacific Economic Cooperation. (2005). *APEC Privacy Framework.* Retrieved 6 July 2025, from https: //www.apec.org/publications/2005/12/apec-privacy-framework
[17] Rong, K., Ling, Y., Yang, T., & Huang, C. (2025). Cross-border data transfer: patterns and discrepancies. *Journal of International Business Policy*, 1–23.
[18] Schwartz, P. M. (2018). Legal access to the global cloud. *Columbia Law Review*, *118*(6), 1681–1762.
[19] Kuner, C. (2023). Data and extraterritoriality. *In Research Handbook on Extraterritoriality in International Law* (pp. 356–371). Edward Elgar Publishing.
[20] Stavridou, V. (2024). *Balancing Sovereignty and Integration: Digital Policy Dynamics in the European Union.* https://www.uppsatser.se/uppsats/cf0b1712c0/
[21] Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, *34*(1), 134–153.
[22] He, X. (2024). EU Data Governance Act: New Developments in Data Governance Rules and Implications for China. *Mod. L. Rsch., 5*, 11.
[23] Guo, S., & Li, X. (2025). Cross-border data flow in China: Shifting from restriction to relaxation? *Computer Law & Security Review*, *56*, 106079.
[24] Yang, X. (2021). Regulatory approaches of cross-border data flow in the big data era: china's choice (Vol. 1848, p. 012026). Presented at the *Journal of Physics: Conference Series,* IOP Publishing.
[25] Chen, S. (2021). Research on data sovereignty rules in cross-border data flow and Chinese solution. *US-China L. Rev.*, *18*, 261.
[26] Chen B., & Wang B. (2024). Legal Regulation and Improvement of China's Data Export from Sovereign Perspective. *Journal of Huaqiao University (Philosophy and Social Sciences Edition)*, *2*, 49–63.
[27] Ye C., & Yan W. (2024). Current Situation, Problems and Relief Paths of China's Cross-border Data System. *Journal of Beijing University of Aeronautics and Astronautics (Social Sciences Edition)*, *1*, 57–71.
[28] Xu D. (2018). International Pattern of Personal Data Cross-border Flow Regulation and China's Response. *Legal Forum*, *3*, 130–137.
[29] Yang T. (2004). EU Digital Economy Governance and Its Implications for China. *China Policy Review*, *5*, 88–100.