Cross-Border Data Issues in International Trade: Legal Challenges, Response Strategies, and Future Prospects

Tongnan Lin

University of International Business and Economics, Beijing, 100029, China
202209015@uibe.edu.cn

Abstract. In the field of international trade, cross-border data flows now have an increasing impact on the global economy. Though data transfers can bring great benefits to countries, it is worth noting that there are still some issues that remain unsolved, which may impede national interests without proper regulation. This paper first analyzes the global status of cross-border data trade, including the current state, growth trends, and major challenges. It is easy to see that problems are concentrated on legal and regulatory differences, data security and privacy protection, and national security. Currently, there are two methods to cope with the issues, extraterritorial jurisdiction and data localization. In order to conduct an in-depth analysis of each strategy, two cases will be discussed in the passage: one is data flow legislations in the US and the EU, and the other is China's requirements for data localization. After a comparative analysis of case lessons and impacts, some recommendations will be provided for the legal framework of cross-border data flows in international trade, such as pathways for international coordination and cooperation, certifications from specialized institutions, and the establishment of a unified guarantee system. At the end of the essay are the future prospects for cross-border data rules in international trade.

Keywords: Cross-Border Data Flows, Extraterritorial Jurisdiction, Data Localization.

1 Introduction

With the advancement of the Internet, cloud computing, big data, and other next-generation information technology, there is a growing need for cross-border data exchange, which has changed the traditional pattern of the world economy and international trade. In the context of increasingly globalized digital markets, international data transfers now play an instrumental role in the global economy. According to the Brookings Institution, cross-border data flows contributed 10.1 percent of global economic growth in the decade 2009-2018 and are expected to reach $11 trillion by 2025 [1]. However, problems raised by cross-border data flows are rather complicated and hard to tackle, such as inadequate legislation, different supervision mechanisms, and national security risks. Divergent regulations on data privacy, data sovereignty, and

B. Siuta-Tokarska et al. (eds.), *Proceedings of the 2024 2nd International Conference on Management Innovation and Economy Development (MIED 2024)*, Advances in Economics, Business and Management Research 300,
https://doi.org/10.2991/978-94-6463-542-3_44

cybersecurity pose significant barriers, complicating the transnational operations of businesses and raising concerns about the protection of individual rights.

This paper responds to these challenges by analyzing existing legal structures, assessing the adequacy of current response strategies by governments and corporations, and anticipating future legal developments in the digital trade landscape. The significance of this paper is multi-fold. Economically, understanding and navigating cross-border data flows is pivotal for maintaining the competitiveness of enterprises in the global market. Legally, it raises questions about jurisdiction, enforceability of laws across borders, and the reconciliation of conflicting national legal frameworks. Ethically, it touches upon the safeguarding of personal data privacy in a world where geographic boundaries are increasingly irrelevant.

The structure of the paper is designed to guide readers through a logical progression of topics. Part 1 will analyze the global status and challenges of data cross-border trade. Part 2 will investigate the data flow dispute between the EU and the US and China's localization demands on data. Part 3 will propose actionable response strategies and a framework for legal reforms. Part 4 will encapsulate the key findings and contributions of the research.

2 The Global Status and Challenges of Cross-Border Data Trade

2.1 The Current State of Cross-Border Data Flows

It has been expressed as far back as the 1998 Work Programme on Electronic Commerce of WTO that all areas of trade would be deeply affected by the Internet, especially the trading rules for goods, services, and intellectual property (IP) rights [2]. While, given a relatively low level of technical skills at that time, the dual mobilization of policy and scholarship proposed by the WTO membership did not work well.

Nowadays, the impacts of data collection, storage, and transfer upon personal privacy and national security are particularly recognized by scholars and policy-makers, which has led to reform of related laws such as data protection and privacy laws and regulations around the world. The EU General Data Protection Regulation (GDPR) is a case in point. Besides, after the legal adaptation under the umbrella of the WTO has stalled, many countries turn to address cross-border data issues in preferential agreements, either of a bilateral or regional nature. According to the Trade Agreements Provisions on Electronic-commerce and Data (TAPED), among the 375 free trade agreements (FTAs) signed between 2000 and June 2022, 137 contain provisions on digital trade and 105 have dedicated electronic commerce or digital trade chapters [3].

2.2 Growth Trends of Global Data Flows

It is well recognized by the international community that despite yielding benefits, cross-border data flows could adversely affect personal privacy and national security. Generally speaking, developed countries like the United States advocate the free flow

of data, while new trends in domestic and international laws have emerged for the purposes of protecting digital assets and maintaining administrative authority and judicial power.

Restrictive Measures on International Data Transfers.

Concerning the mass scale of data exchange, it is nearly impossible for regulatory agencies to cover every aspect. Under such circumstances, disordered data flows may inevitably challenge a state's national security interests, regulatory frameworks, and even enforcement powers. In order to preserve national sovereignty and achieve public policy objectives, some countries turn to pursue restrictive policies and strategies on cross-border data flows. No matter in an international forum like G20 or a bilateral free trade agreement (BFTA), there are always limitations on data exchange, and the demand for localization never goes away.

Flexible Policies on Sensitive Data.

To address the diverse nature of data and associated risks, many countries are experimenting with flexible policies tailored to specific data classifications. For example, France demands the local storage of data in the field of governmental administration, business development, and tax; Australia explicitly prohibits the exit of health data; the United States forbid any safety-related data to be stored in the public cloud; Korea asks telecommunication services to take measures to cut the data flows in economy, industry and technology, and so on.

Exacerbating Conflicts Between Data Sovereignty and Long-arm Statute.

In the realm of the digital economy, reliance on cross-border data flows is intensifying the global contest for cyber and data resources. While the US and Europe often employ aggressive strategies to extend their jurisdiction through extraterritorial statutes, emerging economies like China and Russia emphasize data sovereignty and localization, thereby reflecting a defensive stance on data exchange. These divergent approaches amplify the conflict between the principles of data sovereignty and the assertion of jurisdictional reach, posing challenges for the harmonization of international data trade laws.

2.3 Major Challenges

Legal and Regulatory Differences.

With the global development of the digital economy, each country has set up new policies to regulate cross-border data flows. Though liberal rules are conducive to international trade, they may increase the difficulty of risk-control, which can potentially harm the national interests of developing countries and provide chances for developed countries to control the global economy. Restrictive rules can help developing countries mitigate the potential risks and resist data hegemony but inevitably weaken the economy at the same time [4].

Influenced by a variety of factors including geopolitics, national security, privacy protection, and the level of economic development, many countries have adopted different policies to regulate data flows. A case in point is the United States, with its implementation of the CLOUD Act (Clarify Lawful Overseas Use of Data), which embodies a shift in the locus of data jurisdiction from the physical servers to the entities that manage and control the data, thereby extending legal reach beyond its borders. This legislative move underpins the US strategy to navigate the global digital landscape authoritatively. In sharp contrast, countries like Vietnam have instituted measures that compel international tech companies to invest in local data infrastructures as a prerequisite for market access. Similarly, Russia's insistence on domestic data storage as a precursor to international data transfer embodies a defensive legal posture aimed at maintaining data within its jurisdictional reach.

Data Security and Privacy Protection.

The involvement of sensitive personal information is almost inevitable in digital commerce. According to the EU's GDPR, personal information can be divided into general information and sensitive information. Sensitive information refers to personal information that may lead to discrimination or serious threats to one's safety and property, including religious belief, health status, bank card numbers, home address, etc.

In contexts like cross-border commerce and healthcare, the exit of such sensitive personal information is the prerequisite for convenience and quality services. However, if the data recipients lack sufficient protection of privacy or misuse such data, they may infringe upon individuals' right to privacy. This is best exemplified by Facebook, which collected and stored sensitive information of its users but failed to take effective security measures which finally led to a serious leakage. In 2018, Facebook faced significant backlash when the Cambridge Analytica scandal revealed the mishandling of user data, affecting approximately 87 million users, primarily in the United States [5].

Unfortunately, there is no well-recognized privacy security system in international law. Given that the security criteria are quite different in different areas, the protection gaps are hard to avoid. Even though international coordination and cooperation at all levels is ongoing to solve the problem, the influence is limited to FTAs between countries and regions [6]. Besides, the Cross-Border Privacy Rules (CBPR) developed by the governmental international organization Asia-Pacific Economic Cooperation (APEC) are merely advocacy standards and have not been accepted as general guidelines of the international community.

National Security.

The sources of national security threats in cross-border data flows can be classified into two categories: the exit of personal data and non-personal data.

Risks in the exit of personal data are mainly reflected in political and cultural security. It is noteworthy that with some special skills, data controllers are able to track individuals through data, which means they can influence target people. In this way, a

large number of people are exposed to ill intentions. For instance, overseas political organizations can propagandize the public based on their needs and preferences collected from personal data, and thus get them to vote for a particular candidate.

Threats posed by the exit of non-personal data mainly come from map data, registry data on immovable property, and biological data. High-accuracy map is the basis of national defense, and most countries conduct rigorous monitoring of map data. However, the original data collected by automobile enterprises has far exceeded the prescribed accuracy, which includes confidential information such as breadth and slope [7]. Similarly, land data about the terrain and geographic location is recorded on the immovable property registry [8]. With the above data, it is easy to make a chart of the geographical coordinates of a country, which will definitely threaten homeland and military security. Needless to say, the leakage of biological data can cause disastrous results, best exemplified by the notorious biological weapons.

3 Case Studies on Cross-Border Data Flows in International Trade

3.1 Criteria and Reasons for Case Selection

Today, in the context of cross-border data flows, problems of traditional jurisdiction in data governance are well recognized. Since internet service providers and servers are under the domain of foreign countries, data generated by local users is stored outside domestic jurisdiction. Nevertheless, international law enforcement cooperation and judicial assistance are not enough to solve the problem. Current solutions can be categorized as follows: expanding the jurisdiction or localizing the cross-border data.

Since there is no limitation on a country's scope of jurisdiction in customary international law, some developed countries extend the application of domestic law to overseas persons, property, and behavior through extensive interpretations of the provisions [9]. The United States and the European Union are the most eminent representatives, though they achieve the goal in quite different ways, both the CLOUD Act and the GDPR have a profound influence on the international community, and there will be a further discussion about them in the next part.

The localization of data is the other coping strategy for cross-border data issues. With restrictions on data exchange, exclusive jurisdiction over data can be achieved within the country, and any country that wants to exercise its extraterritorial jurisdiction must have the consent. While localization is also a two-edged sword: it ensures data sovereignty indeed, but hinders economic growth and reduces the efficiency of international cooperation. Considering China's developed Internet industry and its great influence around the globe, China's requirements for data localization will be taken as the second case study.

3.2 Case Study 1: Data Flow Legislations in the US and the EU

Background and Points of Dispute.

It has been a long time that the United States have a decided advantage in data control and thus force others to follow the rules created by them. For example, according to the CLOUD Act, as soon as the United States reach an "agreement" with other countries, the US government can lawfully access the data stored in foreign servers without authority. In this way, the US successfully expands its jurisdiction to another country.

Compared to America, the Internet industry of the European Union is far from competing with the former. As foreign Internet services have a considerable share of the EU market, there is little space for local enterprises to grow. Even worse, a large amount of EU data is stored overseas, under the governance of other countries, and the EU itself has relatively weak control over personal data. The above factors lead to a dilemma: on the one hand, if the EU puts restrictions on the development of the local data industry, chances are that it will miss out on a new economic growth point; on the other hand, the EU will be at a disadvantage if it follows the rules of America [10].

To break the dilemma, the European Union actively promotes the free flow of data among the member states, striving for the formation of a unilateral digital market. Meanwhile, the EU applies strong controls over the exit of data and establishes common standards for data protection with the application of the extraterritorial provisions of the GDPR. As a result, the EU has now successfully strengthened its capacity of personal data control and limited foreign Internet companies.

Application and Effects of the Legal Framework.

The US CLOUD Act extends data sovereignty into technological practices, impacting both domestic and international entities. It applies to US jurisdiction entities, including American companies, foreign firms operating in the US, and their interactions with data, such as possession and control, regardless of the data's location. The Act categorizes entities as providers of electronic communication services (ECS) or remote computing services (RCS), covering a broad spectrum from email services to social media platforms. Under this legislation, these providers must comply with US government requests for data, even if it is stored overseas, challenging traditional notions of data sovereignty. To address potential conflicts with foreign data laws, the Act allows certain foreign governments direct data access within the US without prior consent, subject to stringent criteria set by the US This provision alters the landscape of international data exchange, linking it closely with digital diplomacy and trade negotiations.

Meanwhile, the EU's GDPR incorporates extraterritorial provisions that extend its reach beyond EU borders, pivotal for global trade and digital commerce. This reach is defined through two primary standards: the "establishment standard" and the "relevance standard". Under the establishment standard, the GDPR applies to data controllers or processors—entities determining the purpose and means of processing personal data—established in the EU. An establishment in the EU does not hinge on the size

or staff count but requires stable arrangements and genuine, effective business activities within the Union [11]. The relevance standard broadens GDPR's scope to entities outside the EU engaging in data processing activities related to offering goods or services to, or monitoring the behavior of, individuals within the EU. This standard ensures that non-EU businesses engaging with EU markets comply with GDPR. The European Data Protection Board (EDPB) seeks to refine these standards' application, emphasizing the link between data processing activities and an EU establishment. A mere nominal presence in the EU does not suffice; there must be a significant connection between the data processing activities and the EU establishment for GDPR to apply. Similarly, incidental or accidental targeting of individuals in the EU does not fall under GDPR jurisdiction, indicating a nuanced approach to its extraterritorial reach.

Case Lessons and Impacts.

The US CLOUD Act has enhanced global data flow, securing agreements like the UK-USA Data Access Agreement and support from tech giants, despite necessitating national sovereignty compromises and domestic law adjustments in participating countries. In contrast, the EU's GDPR has profoundly influenced global data protection standards, becoming a model for countries worldwide due to its comprehensive personal data protection and cross-border transfer safeguards. While the CLOUD Act focuses on facilitating data access, GDPR emphasizes privacy and protection, reflecting divergent approaches to international data governance. In fact, countries outside the EU and US are adopting similar regulations, contributing to a more fragmented digital landscape requiring multinational companies to navigate a patchwork of laws.

Data flow disputes affect not only legal compliance but also international trade. Companies must reassess their data handling and storage practices, potentially impacting cloud services, e-commerce, and digital trade. The emphasis on data localization and sovereignty could lead to increased operational costs and challenges in global market access. Additionally, the tensions between the EU and US over data governance call for enhanced international dialogue and cooperation. Developing a framework for mutual recognition of data protection standards or a global treaty on data flows could mitigate conflicts and support the growth of the digital economy.

3.3 Case Study 2: China's Requirements for Data Localization

Background.

The essence of data localization lies in the restriction of cross-border data so that it can be co 0ntrolled within a country. There are many ways to achieve the goal, such as storage in a domestic server, prior consent of data subject, and data export duty, etc [12]. Among them, the localization of data is the most important manifestation of territorial jurisdiction, which is also the data strategy of China to deal with the extraterritorial jurisdiction of US and EU.

Initially, China's regulations on cross-border data issues were fragmented at the legislative level, scattered in criminal, civil and administrative laws, which led to a

narrow scope of application [13]. Since there was no specialized law to ensure the enforcement, some provisions even lacked legally binding effect, resulting in management turmoil of data governance.

Legal Framework and Application.

China's approach to managing cross-border data flows integrates tightly with its broader objectives in international trade and cybersecurity, anchored by three pivotal laws: the Cybersecurity Law, Data Security Law, and Personal Information Protection Law.

As the first law to regulate issues of cyberspace security, the Cybersecurity Law requires a security assessment of cross-border data flows. After that, Measures for the Security Assessment of Outbound Data Transfer determines the subjects as personal information and important data, which are also the key concerns of protection and supervision. The regulatory regime demands network service providers to set up a domestic server, and the exit of data must be reviewed by a national agency.

Based on the National Security Law and the Cybersecurity Law, Data Security Law defines some terms from a legal perspective including "data", "data processing", and "data security", which has laid the foundation for data governance. Given that data collected by different entities such as governments, enterprises, and institutions are far from each other, their requirements for assessment and protection are not the same, the Data Security Law has made clear provisions on this issue. Besides, in order to regulate data processing activity and ensure data security, a protection system based on data classification is established, which can promote the application of data in the meantime.

The introduction of Personal Information Protection Law has strengthened personal data protection in China. For example, the scope of data protection extends to foreign countries, and personal information is distinguished as sensitive and non-sensitive, which also clarifies the range of data review. Besides, considering the separate consent principle, the individual's consent is also a must in data flows [14]. To sum up, the Personal Information Protection Law not only promotes healthy development of the digital economy, but safeguards the rights and interests of citizens as well, which also marks a new level of China's personal information protection and complies with international standards.

Case Lessons and Impacts.

Collectively, these laws signify China's strategic positioning in the global digital economy. They serve dual purposes: safeguarding national security and personal privacy, and crafting a regulatory environment conducive to international trade and digital commerce. The case of China's data governance framework exemplifies the role of data sovereignty in shaping international relations and trade policies. It highlights the potential for data protection laws to act as both barriers and facilitators of international trade, depending on their design and implementation. By covering various facets of data security and personal information protection, these laws enable China to

control its digital environment effectively, setting a precedent for how countries can manage their cyber and data security while engaging in international trade.

For international businesses, China's data governance laws necessitate stringent compliance strategies to operate within its digital economy. The requirement for data localization and the obligation to undergo security assessments before transferring data internationally can influence global data management practices and operational costs. By establishing clear rules for data usage and protection, China aims to create a secure environment that fosters innovation and growth within its digital economy. This regulatory certainty can attract investment and stimulate the development of new technologies and services, potentially setting benchmarks for other countries.

4 Legal Framework Recommendations for Cross-Border Data Flows in International Trade

4.1 Pathways for International Coordination and Cooperation

Recognizing the diverse developmental stages of technology, economics, legal systems, and privacy cultures across nations, it becomes imperative to forge pathways for international coordination and cooperation. The CPTPP offers an instructive model in this regard, distinguishing itself from the RCEP by establishing a more inclusive mechanism for data flow management.

With regard to cross-border data issues, CPTPP categorized the data subjects according to commercial and non-commercial use of data. When there is a business purpose, CPTPP requires member states to allow data to flow freely across borders in electronic form. Accordingly, the exception clause is that, for the sake of achieving public policy objectives, restrictive measures are allowed unless there is arbitrary or unjustifiable trade discrimination.

This principle reflects a sophisticated understanding of the complex dynamics at play in the digital era. On one side, it champions the cause of cross-border data activities, recognizing their critical role in driving economic integration and innovation. On the other, it acknowledges the potential risks and challenges posed by unregulated data flows, including issues related to privacy, national security, and economic interests [15]. Therefore, the CPTPP's stance on data flows represents a strategic compromise, which influences in the shaping of global trade rules. By adopting this model, the CPTPP not only facilitates the expansion of digital trade but also sets a precedent for future international agreements, highlighting the importance of flexibility, protection, and cooperation in the governance of cross-border data flows.

4.2 Certifications from Specialized Institutions

From the perspective of trade liberalization and data privacy, it is easy to understand neither individuals nor enterprises want to be restricted by public power, which also explains why the security assessment from a national agency is hard to accept [16]. A direct contract may avoid government intervention to some extent, but there are still

problems such as low trust in online transactions and the lack of confidentiality safeguards.

As a result, transacting through specialized institutions is regarded as a compromise approach. Such certifications provide a preliminary basis for trust between parties by signaling compliance with established legal, security, and privacy standards. They serve as indicators of an entity's commitment to maintaining data integrity and safeguarding against breaches, thereby facilitating smoother initial interactions in cross-border data transactions. Apart from that, specialized institutions are able to guarantee legal, safe, and orderly trading in the international field. Being independent from the administrative organs, such institutions can play a third-party role and remain neutral, so that their professionalism and fairness are accepted by a wide range of cross-border data processors [17].

4.3 Unified Guarantee System

The underlying conflict of cross-border data regulations is rooted in the growing mistrust among countries. There are two contradictory trends in the international community. One is among countries at different stages of development. Developed countries fear that data flows to developing countries will not be properly protected and used, while developing countries are in doubt that developed countries will overexploite the collected data, which may pose a threat to their national security. The other is among countries at the same stage of development but have different rules. A case in point is the "Prism Gate" incident, which destroyed the confidence between the US and EU, and finally led to the repeal of the US - EU Safe Harbor Framework [18].

In light of these challenges, the establishment of a unified guarantee system—a global data community with shared destinies and responsibilities—is proposed. Such a system, endorsed by entities including the United Nations, aims to bridge the trust gap among countries by fostering a consensus on the principles and practices that should govern international data flows. A unified approach to data governance would not only alleviate the current climate of suspicion but also lay the groundwork for enhanced cooperation and mutual understanding among nations. To actualize this vision, it is imperative for all countries to engage in the creation of legal frameworks centered on unified guarantees for data flows. These frameworks should prioritize the harmonization of data protection standards, ensuring that data flows freely yet securely across borders, thereby supporting the flourishing of international trade in the digital era.

4.4 Future Prospects

The cross-border data mechanism should be a long-term program and constantly adjusted. Whenever there is a change in inter-state relationships or a new breakthrough in high technology, it might often be the case that the current legislation will be continuously amended to respond to the emerging needs and problems.

Though the US and EU models have already taken the lead in the establishment of cross-border data rules, it is worth noting that a large number of developing countries

especially those lagged behind are in urgent need of resources, policies, and international environment to create, nurture and develop their own digital industries, and billions of people have not accessed the Internet yet. However, the lagging countries are at a distinct disadvantage in the current digital industry, they need time to build data infrastructures, fill capacity gaps, and support domestic enterprises, while the US and EU models leave no room for them. Such problems have yet to be resolved, therefore, the demands and interests of the latecomers should be taken into account when dealing with cross-border data issues in future.

To this end, technological solutions play a pivotal role. Innovations such as distributed ledger technologies (e.g., blockchain) offer promising avenues for enhancing data integrity and security while facilitating transparent, efficient cross-border data flows. Additionally, the deployment of advanced data analytics and artificial intelligence can help nations optimize their data governance practices, enabling them to leapfrog traditional developmental barriers. However, the successful implementation of these technologies requires a concerted effort to enhance digital literacy, build technical capacity, and ensure equitable access to technology across the globe.

5 Conclusion

This paper conducts deep research into the issues of cross-border data flows, focusing on the specific challenges and the response strategies. Learning from the cases of the US, the EU, and China, all the problems related to international data regulations stem from the differences in legal frameworks. Developed countries want to expand their jurisdiction through free data flows, some countries follow their rules, while others use the localization strategy to preserve their data sovereignty.

In short, the real question behind regulating conflicts is national interests as well as international relations. Therefore, in order to make the best use of cross-border data flows, it is necessary to bridge the trust gap among countries, which can also lay the groundwork for enhanced cooperation and win-win results. The establishment of a unified guarantee system can be a possible approach, or at least introducing some specialized institutions to reconcile the relationship as the third party. To sum up, the key to cross-border data issues lies in not only the legal frameworks but also the national interests. With the gradual change of the international community and the advancement of high technology, rules for data flows will remain challenging and be constantly adjusted to new needs.

References

1. Joshua P. Meltzer., Peter Lovelock.: Regulating for a digital economy–understanding the importance of cross–border data flows in Asia. Global economy&development working paper, 113 (2018).
2. World Trade Organization, https: //docs. wto. org/ dol2fe/ Pages/SS/ directdoc. aspx? filename=Q:/WT/L/274.pdf&Open=True, last accessed 2024/4/10.

3. Rodrigo Polanco., Mira Burri.: Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset. Journal of International Economic Law 23(1), 1–34 (2019).
4. Qijia Ma., Xiaonan Li.: China's Legal Framework for Regulating Cross–border Data Flows. Research on Rule of Law 1, 91–101 (2021).
5. Huan Zhang., Ming Wen., Youhai Wang.: On Legal Protection of Personal Information from "Facebook" Data Abuse Incident. Journal of Chongqing University of Posts and Telecommunications(Social Science Edition) 30(6), 56–63 (2018).
6. Sheng Zhang.: Cross-Border Data Flows in the Framework of International Investment Law:Protection, Exceptions and Challenges. Contemporary Law Review 33(5), 148–160 (2019).
7. Zongren Jia.: Maps in self-driving cars. China Surveying and Mapping 4, 27–31 (2019).
8. Weiying Wang., Lanlan Zhu.:Analysis on Information Risks of Real Estate Registration Files. Archives Management 3, 57–58 (2020).
9. Jian Jiang.: Extraterritorial jurisdiction of US and European data legislation and China's response——Centered on the Cloud Act and GDPR. Tianjin University (2021).
10. Kairu Ye.: "Long–Arm Jurisdiction" in Data Flow Regulation: Originalist Study on GDPR of EU. Law Review 38(1), 106–117 (2020).
11. Haijing Ao.: Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3). Business and Economic Law Review 2, 135–158 (2020).
12. Anupam Chander.: Data Nationalism. Emory law journal, 679–704 (2015).
13. Ning Huang.: Impacts of Data Localization and Its Policy Motivations. Forum on Science and Technology in China 9, 161–168 (2017).
14. Yufei Yan.: The Research on legal regulation of Data Outbound Rules in China. Southwest University of Science and Technology (2023).
15. Mira Burri.: Cross–border data flows and privacy in global trade law: has trade trumped data protection?. Oxford Review of Economic Policy 39(1), 85–97 (2023).
16. Guoqi Zhang., Chen Wei.: Domestic Rule System for Cross–border Data Flow. Journal of Karamay 14(2), 77–84 (2024).
17. Duoqi Xu.: Legal Guarantee for Two-way Compliance of Enterprises Subject to Regulation of Cross–border Data Flow. Oriental Law 2, 185–197 (2020).
18. Ran Tao.: Analysis and revelation of cross border data strategic gaming between the US and the EU. China Economic&Trade Herald 2, 30–33 (2024).