Risk Prevention and Response to Cross-Border Data Flows in the Context of National

Xinzhu Tian

Northwest University of Political Science and Law, Xi'an 710063, China.

Abstract: The storage, use and circulation of data cross national borders, making digital trade possible, and the centrality of data continues to be highlighted, with countries around the world engaging in fierce games in the field of cross-border data flows. Based on the security risks of cross-border data flows and facing the dual dilemmas of domestic and international governance of cross-border data flows, the limitations of China's current domestic legal system for cross-border data flows and its compatibility with The study analyzes the limitations of China's current domestic legal regime for cross-border data flows and the compatibility with international rules. In this regard, there is an urgent need to build a dynamic two-way regulatory system for cross-border data flows through blockchain empowerment, refine the Data Exit Assessment Methodology, connect with international "security exception" provisions, advocate for a cyber community of destiny, strengthen extraterritorial cooperation, and promote the exploration of global governance solutions for cross-border data flows.

Keywords: Cross-Border Data Flow; Data Localization; Security Exception Clause; Blockchain Technology

1. Introduction

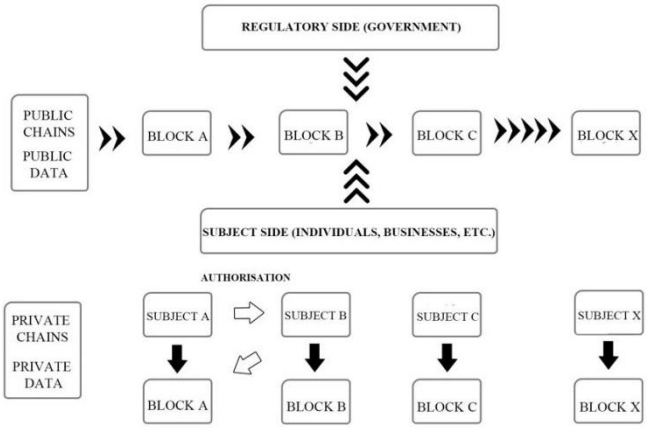
The digital economy is developing at an unprecedented pace, radiating widely and having an unprecedented degree of influence, and is becoming a key force in restructuring global factor resources, reshaping the global economic structure and changing the global competitive landscape. Developed countries led by the US and the EU are actively promoting a new pattern of international governance led by them, including the signing of the Comprehensive and Progressive Trans-Pacific Partnership Agreement (CPTPP) and the Digital Economy Partnership Agreement (DEPA), marking a higher demand for the freedom of cross-border data flow by developed countries led by the US, but the current economic and technological and legal system level between China and However, the current gap between China and developed countries at the level of economic technology and legal system makes China show defensive characteristics on the issue of regulation of cross-border data flow, adopting the data localization model and taking safeguarding data sovereignty and security as the primary principle.

2. Chinese Solutions to Prevent The Risk of Cross-border Data Flows

2.1 Apply blockchain technology

With national security as the value orientation, Article 24 of China's Data Security Law provides for a security review system for important data leaving the country, so that data that is highly relevant to national interests and people's interests can be inspected as much as possible. This is not just a slogan, but the challenges faced by China at present are at the levels of technical recognition and legal regulation. Therefore, to build a dynamic two-way data exit regulation system based on "technology + law" through blockchain-enabled data cross-border flow regulation is an effective means to address the current challenges of legal regulation in China. This is an effective means to address the current challenges of domestic legal regulation.

Figure 1 Blockchain regulation diagram.



Blockchain enables data security monitoring (see Figure 1). On the one hand, blockchain technology has the technical advantages of monitoring data trajectories, data traceability, anti-tampering and secure and efficient data sharing and flow, specifying the responsibilities of the National Data Bureau as the supervisory end, monitoring the nodes of data flow, determining the time of nodes, based on cryptographic algorithms and network technology, preventing data intrusion and data tampering through data traceability and node monitoring, and analyzing the data flow in real time. This will help to monitor the flow of data from the source and prevent the government from falling into the deadlock of "headless" regulation. On the other hand, both individuals and enterprises can link data through any node as the subject end, realizing the data operation mode among multiple subjects. Enterprises can store their own data by means of a private data chain, and the security of the data stored on the subject side of the blockchain can be ensured through blockchain authentication, tamper-proof and traceability technology. In addition, through blockchain technology, data stored in the chain can be encrypted and access rights can be set. Access to other people's data needs to be applied for by applying to the party to whom the data private chain belongs, and both parties can determine the access rights and scope by entering into a contract and backing up authentication, so as to guarantee the data security of the subject within the scope of the blockchain.

2.2 Alignment of International Rules

China's signing of the RCEP is the first example of China's practice on cross-border data flows in the international arena, and it has opened up a new way of thinking for China to explore the extraterritorial governance system for cross-border data flows. However, an objective assessment of the gap between the "security exception" clause in the RCEP and the CPTPP agreement developed by developed countries, as well as the effective interface between China's domestic legal system and international rules and regulations, requires China to take a more cautious approach to its participation in the development of global solutions for cross-border data flows, and to look rationally at its cooperation with developed countries. China should take a more cautious approach to its participation in the formulation of the global scheme on cross-border data flows, and take a rational view of the gap between China and developed countries in terms of the technical aspects and legal system of cross-level data flows, so as to avoid the impact on China's data sovereignty and security due to excessive steps in the formulation of international rules. First, the CPTPP imposes strict limitations on the power of each Contracting Party to exercise discretion in the exercise of "security exceptions", i.e. it does not support the exercise of discretion by Contracting Parties over adverse restrictions on digital trade and restrictive or prohibitive measures that undermine the flow of data across borders. The restrictions on the exercise of discretion under the "security exception" in the US have placed greater demands on China's regulatory system for cross-border data flows after its accession to the CPTPP. Therefore, it is necessary to clarify the scope of application of the "fundamental security interests" in the CPTPP and the principles to be invoked, further refine China's domestic Data Exit Security Assessment Measures, and promote its harmonization with the higher standard CPTPP exception clause on "fundamental security interests". This will constitute a reasonable basis for invoking the "security exception" clause at the international level. Secondly, with regard to the RCEP signed by China, which is a multilateral agreement on cross-border data flows with many developing countries based on the need for their own data sovereignty and security, it is necessary to further improve the conditions for the application of the security exception clause in the agreement and gradually increase the level of openness of cross-border data flows on the basis of safeguarding the overall situation of China's data sovereignty and security.

2.3 Strengthen Regional Cooperation

In recent years, China has paid great attention to and actively participated in the negotiation of international rules on data, adhered to the sovereignty and security of data, signed the Regional Comprehensive Economic Relations Agreement, and issued the "China+5 Central Asian Countries" Data Security Cooperation Initiative. In the process of bilateral and multilateral consultations with other countries, China will demonstrate its determination to join hands with other countries to build a community of cyber destiny, and continuously expand the breadth and depth of application of international rules on cross-border data flows in China. On the other hand, China should accelerate the negotiation process with key regions and countries on cross-border data flows, build on the Global Data Security Initiative, and make use of its friendly and cooperative relations with members of the Shanghai Economic Cooperation Organization, the BRICS and ASEAN regional countries to vigorously promote cross-border data flows among key regions; at the same time, we should strengthen exchanges with the "Belt and Road "At the same time, we should strengthen exchanges with countries along the Belt and Road, and conduct discussions and studies on the cross-border flow of data among countries along the Belt and Road as soon as possible, so as to form a mechanism for the cross-border flow of data. As an advocate of the "Belt and Road" initiative, China should take up the responsibilities and obligations of a country when formulating the cross-border information circulation mechanism of the "Belt and Road", adhering to the principles of "peace and cooperation, openness and tolerance, mutual learning and learning, mutual benefit and win-win". In the "Silk Road Spirit", we should promote international cooperation in the "One Belt, One Road" area and establish a multilateral cooperation mechanism.

3. Conclusion

With the development of the digital economy, international digital trade is becoming more and more frequent. The risk to national security posed by the cross-border flow of data has become increasingly prominent. We are still at the preliminary stage of exploration in the management of cross-border flow of data. Therefore, based on the Data Exit Security Assessment Measures and supported by blockchain technology, we will further improve China's data exit classification standards and promote a two-way transformation of "technology + institution", thus opening up a new way for effective interface between China's data cross-border flow regulations and the norms and standards of international regional agreements. Building on the Global Data Security Initiative, common consultation, sharing and collaboration with countries in key regions is key to establishing a new model for cross-border data management.

References

[1] Dimitropoulos G. Chaisse J. (2023). ‘The Black Pit:’ Power and Pitfalls of Digital FDI and Cross-Border Data Flows. World Trade Review, no. 1, pp, 73-89.

[2] Huang G and Lei Y. (2022). The Norms on Cross-Border Data Flows in the RCEP. Asian Journal of Law and Economics, no. 3, pp. 375-404.

[3] Wang AN. (2022). Challenges faced by Russian companies involved in cross-border data flows. The Frontiers of Society, no. 7.

[4] Chin YC and Zhao JW. (2022). Governing Cross-Border Data Flows: International Trade Agreements and Their Limits, no. 4, pp. 63-63.

[5] Gregory VW. (2022). Cross-Border Data Flows, the GDPR, and Data Governance. International Organizations Research Journal, no. 1.

[6] Jiang XD. (2022). Governing Cross-Border Data Flows: China’s Proposal and Practice. China Quarterly of International Strategic Studies, no. 1.

[7] Yang X. (2021). Regulatory Approaches of Cross-border Data Flow in the Big Data Era: China’s Choice. Journal of Physics: Conference Series, no. 1.

[8] Quan XL. (2020). The Governance of Cross-Border Data Flows in Trade Agreements: Is the Cptpp Framework an Ideal Way Out?. Frontiers of Law in China, no. 3, pp. 253-279.

[9] Mitchell AD and Mishra N. (2019). Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute. Journal of International Economic Law, no. 3, pp. 389-416.