Pacific International Journal, Vol. 6(1), 138-141; 2023
ISSN (Print) 2663-8991, ISSN (Online) 2616-4825
DOI: 10.55014/pij.v6i1.326
https://rclss.com/index.php/pij

Security and Openness: China's Cross-Border Data Flow Scheme

Xinyi Du[1], Aijiao Liu[2]

[1.] First author, Baize Institute for strategy studies, Southwest University of Political Science and Law, P. R. China.
[2.] Corresponding author, Baize Institute for strategy studies, Southwest University of Political Science and Law, P. R. China.
Email: duxinyiwork@163.com, 374296511@qq.com

Abstract: Cross-border data flow legislation is currently absent in several countries, and data ownership remains an issue. Data sovereignty is necessary for cross-border data movement. To preserve national interests in the growing data field, western countries violate the idea of sovereignty and attempt to construct a cross-border data circulation system within the framework of the western discourse system. Developing countries aim to localize data to protect their own data stockpiles and increments to safeguard national security. As a responsible country, China supports the formation of a cross-border data flow rule framework that aligns with development and security, protects data sovereignty, and promotes data integrity.

Keywords: China, Global Security Initiative, core content, practical approach

1. Introduction

Numbers have become fundamental resources, ushering in a new era of social and economic revolution. With the advancement of digital technology, data has become a significant productive force and crucial production element, and cross-border data movement has become more common. On this basis, many nations and international organizations have implemented necessary legal systems and built overall coordinating structures. Since 2016, digital trade agreements led by the United States and the West, such as the Comprehensive and Progressive Trans-Pacific Partnership Agreement (CPTPP) and the Digital Economy Partnership Agreement (DEPA), have begun to include rules for cross-border data flow. However, these rules are subordinate to trade negotiations that focus on the economic dimension and have not addressed major concerns, such as national security, caused by cross-border data flow. Particularly in recent years, certain nations have attempted to persuade others to engage in exclusive "small circles" and "construct walls and bases" through economic methods. This not only overlooks most nations' genuine concerns, such as China's, but also degrades global governance in a more complicated international situation. The Party's report to the 20th CPC National Congress states that "China actively participates in the reform and construction of the global governance system, practices the concept of global governance of joint venture, joint construction, and sharing, adheres to true multilateralism, promotes the democratization of international relations, and promotes the development of global governance in a more just and rational direction." On one hand, China actively improves domestic legislation, formally applies to join CPTPP and DEPA, actively promotes international cooperation in digital governance, and aspires to "run with" and "run with," which deserves praise. On the other hand, it is also necessary to begin with the common concern of non-economic cross-border data flow, combine our own exploration, propose a new topic framework, and a China plan outside trade negotiations. China should actively promote the reform of the global governance system for cross-border data flow and strive to "lead" in exploring international digital governance rules.

In February 2023, China announced the Overall Layout Plan for the Building of Digital China, which presented the general framework for the creation of digital China. On March 7th, the first session of the 14th National People's Congress endorsed the State Council's institutional reform plan and formed the National Data Bureau. From the "Overall Layout Plan of Digital China Construction" to the work reports of the two sessions, we can see that data is the cornerstone of economic development and social change on the one hand, and China places a high value on numbers and data on the other.

2.Literature Review

The growth of cross-border data. Traditionally, because the cross-border movement of personal data was the key concern, many publications referred to "cross-border flow of personal data" as "cross-border data flow”. [1] The Computer Application Working Group (CUG) of the OCED Science and Technology Policy Committee (CSTP) proposed the first notion of "cross-border data flow" in the 1970s. In 1980, the Organization for Economic Cooperation and Development (OCED) released the Guidelines on Privacy Protection and Cross-Border Flow of Personal Data (hereafter referred to as the Guidelines), which legally included "cross-border data flow" into legal concerns. As may

[Received 14 Mar 2023; Accepted 23 Mar 2023; Published (online) 31 Mar 2023]

be seen, the applicable restrictions are similarly restricted to the category of personal data. [2] Eventually, as digital technology advanced, "data" was expanded to include more information in the form of "electronic form," rather than only personal data. Nowadays, the majority of cross-border data is personal information data and international trade-related data.

There are three forms of cross-border data flow: data inflow, data outflow, and data retrieval. The presence of national data sovereignty underpins the movement of cross-border data. The first is data intake, often known as data entering. Foreign information enters the domain, and the state has the authority to decide what information enters. National security, public morality or social order, personal privacy protection, domestic law enforcement demands, cultural security, national identity, and ideology are frequently used to regulate data input. Second, there is data outflow, or data leaving the nation. The domain's information flows out of the domain, and data from one nation is acquired by other countries. The most severely restricted type is data departure. The third step is data retrieval. The state institutions of a country forcefully recover non-public material held overseas based on the demands of national law enforcement. Data retrieval include both data entry and data departure. Because it may be represented as two halves of an organic whole. On the one hand, it is demonstrated that domestic organs forcefully access non-public data kept in other nations (data entry), while foreign organs forcibly retrieve non-public data stored in their own countries (data exit).

Regulation of cross-border data flows. Control based on data flow type categorization, that is, control of data exit, control of data entrance, and control of data retrieval, is well understood. The controls are classified according to their policy nature: stiff flow control, flexible flow control, and local backup flow control. [3] Under the strict flow, the prohibition of data leaving the nation is stressed, and Russia and Australia represent robust protection of core and sensitive data. The term "flexible flow control" refers to the ability to relax the limitation on data flow under particular conditions. Its control is centered on the implementation of a safety assessment process, which is represented by the European Union and South Korea. Controlling the local backup flow is a workable method. To realize data circulation and security, all parties are needed to complete the backup in a designated data center situated in China before opening the cross-border circulation of data. India and Indonesia are among them [4]. Yet, cross-border data management and data localization are contentious, as seen by the many notions of data localization. Some academics feel that localized data storage is a policy or law that works against cross-border data movement. Some academics feel that data localization and data departure are distinct institutional architectures. While data localization refers to the storage or processing of data locally, it does not exclude data from being processed in other nations.

3. China's cross-border data flow strategy

EU nations consider their own data protection model to be the standard, and need other countries to follow its regulations before exchanging data with EU countries [5]. The United States, on the other hand, realizes the convergence of data to the United States in the national interest by creating a cross-border data flow model with a low degree of protection. This conduct not only consolidates American firms' worldwide data ownership, but also decreases the regulatory space for data protection in many nations. The practice of limiting the extent of data flow in the United States and Europe runs counter to China's advocacy of global data flow and cross-border data flow.

3.1 A realistic backdrop

Data has evolved into a production element with significant economic worth, entering the stage of data capital. For the first time, data, labor, capital, and land were accepted as components of production to participate in distribution during the 19th CPC Central Committee's Fourth Plenary Session. Yet, data is not valuable in and of itself, and it can only play an essential function when it participates in the production process, hence data has the commodity property. Simultaneously, the bit propagation features of data modify the value law of resource depletion, and the data becomes richer as it is used more frequently. The tension between data transparency and people' right to privacy is becoming more apparent [6]. Capital has the trait of profit-seeking. Since data has economic value, the data is totally dependent on the user's application activity, exacerbating the tension between data openness and individuals' privacy rights. Citizens' right to privacy in a digital culture encompasses not just sensitive data in the conventional sense, but also application behavior. Algorithms stimulate the production of data and create data portraits based on individuals' behaviors in cyberspace. Hence, personal preferences, ideological tendencies, job nature, and so on are gained through the modelling of internet activity. Because data has become the essential condition of the digital society, data-driven businesses will do all in their power to get more data for their goods in order to suit their customers' specific preferences. Data openness is associated with an increase in data risk.

Data is a new field in which sovereign states can compete. As previously said, data ownership is the foundation of digital civilization. Similarly, a country's capacity to assure the stock and growth of data resources, as well as data security, has become a new field of play for sovereign governments. In numerous nations, laws, rules, plans, and policies on "data," "network," and "artificial intelligence" have been released extensively, demonstrating that sovereign governments all aspire to master the right to speak in the field of data.

Data might readily fall under dual jurisdiction in terms of national security. The bottom line of sovereign countries is national security, which is likewise a hazy subject. Because the concept's ambiguity may adapt to the emergence of diverse national interests. As a result, two or more sovereign States may fall into a specific data and claim jurisdiction over the data at the same time for national security reasons [7].

The key to data circulation is secure data exchange. The goal of data security cooperation, whether domestic or international, is to strike a balance between data security and data exchange. Data flows on a regular basis nowadays, yet there are still significant distinctions between data cross-border freedom and data cross-border validity. Meanwhile, data sovereignty is a need for data circulation.

3.2 Cross-border data transfer regulations in various nations throughout the world

Developed nations in the United States and Western Europe have developed a cross-border data flow regulatory framework that serves their own interests. This is reflected in the fact that, in an effort to build an international data ecology centered on the West, American and European countries have continuously strengthened cross-border law enforcement and implemented long-arm jurisdiction based on "national interests" in an effort to build an international data ecology centered on the West. The most common is the "cloud bill," which arose from the 2016 case of the US government v. Microsoft. The "Cloud Act" is an acronym for "Clarifying the Legal Usage of Data Overseas," which the United States issued in 2018. The US Federal Court for the Second Circuit ruled in this case that because the data storage location of users' communication material is in Ireland, Microsoft must extract the data from the Irish data center and "import" it into the United States. The case streamlines the procedure of cross-border data retrieval by the US government, and further establishes the principle of "whoever owns the data has ownership over the data".

Developing economies develop data localization rules based on national security concerns. Data has become a key field of national game as a new arena, and rivalry among major countries is growing increasingly heated. Faced with severe competition, rising nations use data localization rules to secure the security and management of stock data, therefore satisfying their own security requirements. The restrictive policy comprises the following requirements: mandating multinational firms to create data centers in their home countries when conducting business or offering services in their home countries; putting forth localization standards for data storage and server addresses. For example, China's Cyber Security Law requires that personal information and important data collected and generated by key information infrastructure operating in China be stored in China; Russia has a data mirroring policy that requires data to be transmitted and processed abroad but citizens' personal information to be stored and processed on domestic servers.

International organizations strive for the creation of a balanced data ecosystem. Based on the digital transformation trend, the World Organization has given increasing attention to the value of data in recent years. The World Trade Organization, the G20, and the G7 have all signed agreements or declarations aimed at lowering barriers to cross-border data transmission. The International Trade Organization signed the "Joint on E-commerce" in 2019, affirming multilateral e-commerce discussions based on the WTO's current framework. The G20 Digital Economy Ministers' Conference in 2020 focused on data governance and data circulation, and the international community was forcefully urged to promote data connectivity and bridge data circulation discrepancies. The Group of Seven produced a declaration on "digital trade" in 2021, outlining certain criteria of legitimate data transfer.

3.3 Create a cross-border data flow rule system in collaboration with development and security.

Improve the top-level design and introduce the notion of systematic governance. For starters, the formation of the National Data Bureau has strengthened the basis and security of digital China. As a special data coordinating organization, the National Data Bureau has defined three main tasks: coordinating and promoting the construction of digital basic systems, coordinating resource integration, sharing, and development, and coordinating and promoting the planning and construction of digital China, digital economy, and digital society.

Second, cross-border data flow governance should be consistent with the broader national security concept. Coordinate development and security, as well as cross-border data flow and digital economic development. Coordination of domestic and international security, as well as the interaction between domestic data governance and cross-border data flow.

Third, strengthen applicable legislation and provide top-level design papers. In 2020, China launched the Global Data Security Initiative, according to the premise of comprehensive development and security and emphasizing that different subjects should collaborate to construct an orderly cyberspace based on the data sovereignty of all countries. Improve personal data protection, reach bilateral agreements on cross-border data gathering, and promote data integrity. The Data Security Law went into force in 2021, clarifying the data classification protection system, clarifying the exit security management rules of diverse data, establishing exit security review regulations, and making explicit provisions on judicial access to data. After that, China issued the "Measures for the Safety Evaluation of Data Exit" in 2022 to provide explicit institutional procedures for the data exit method of safety assessment.

Fourth, accelerate key technology research and development while cultivating supporting personnel. China's cross-border data flow regulatory approach also sets stricter standards for experts. On the one hand, critical core technical abilities. Independent innovation in science and technology is at the heart of cross-border data flow, and science and technology are the foundation for safeguarding national security. Enhance your fundamental digital technology research skill, fight hard for important core technologies, recognize the beneficial relationship between security and development in the data area, and fully grasp the technological foundation of the digital economy in your own hands. Increase the building of experts and the rule of law team, on the other hand, to fulfil the development demands of the digital industry in the current circumstances. It is required to follow a mix of management system and technical measures, as well as to translate system needs into technical requirements for execution. Create data life-cycle security protection management mechanisms, and improve the filing, protection, detection, and assessment of outgoing data throughout the life cycle. We will increase the capacity building of data security protection technology to ensure the safety of cross-border data flow in light of the cross-border transmission and application requirements of corporate data. In each case, respect data sovereignty and resist long-arm jurisdiction. On the basis of respecting other nations' sovereignty, security, and development interests, China has effectively fostered cross-border data flow through bilateral and multilateral data protection cooperation, releasing the full potential of international cooperation and growth. According to the Global Data Security Initiative, China has a specific requirement for balancing public safety, industry growth, and personal data rights. In principle, it can adopt the approach of "allowing mobility as the major factor localization as the auxiliary factor security assessment exception". Countries should be allowed to develop a hierarchical data supervisory system based on national security, privacy protection, and law enforcement requirements. Urge nations to create and strengthen domestic legislative systems to safeguard personal data security, achieve a clear consensus on each other's data protection level, and construct a multi-channel cross-border data flow mechanism. Maintain national data sovereignty claims, reject unilateral cross-border data access via "long-arm jurisdiction," continue to optimize judicial aid channels, and support the formation of new cross-border assistance mechanisms through bilateral and international agreements.

Integrate actively with international data governance and participate in problem discussion and rule creation. China's active participation in the negotiation of international data laws is predicated on data security and controllability. Provide a dynamic "white list of cross-border data flows" system in accordance with national, regional, and security criteria. To secure digital trade and unfettered data flow, the global digital economy urgently needs new collaboration methods and standards. China should hasten the development of a global cross-border data flow rule framework with Chinese features. Promote scientific and technical collaboration with emerging nations, and employ multilateral structures' convening strength and broad influence to obtain appropriate agreements. Under the framework of the "Belt and Road Initiative" collaboration, efforts will be made to develop data flow protocols and standards, to construct a community of digital space destiny, and to promote a new scenario in global cross-border data flow regulation.

4 Conclusion

Human evolution has progressed to the point of digital civilization. The digital economy has given rise to a shift in state power dynamics and infused digital kinetic energy into human progress. Due of the increased global digital connectivity, humanity not only shared huge advantages, but also incurred great dangers. China has always supported the development of the digital economy, respects various countries' data sovereignty, advocates the establishment of a global and regional development mechanism, strives to turn the world's "risk" into the world's "dividend," and actively promotes China's plans and suggestions for data governance around the world.

Acknowledgements: This article is the phased study result of the "Building the research on social terrorism intelligence analysis and early warning system in the Lancing-Mekong River basin" educational cooperation project of provincial colleges and universities in 2021. (No. SYSX202101).

REFERENCES

[1] Ning Huang, Yang Li. (2017). The Evolutionary Trend of Trans-border Data Flows Regulation and Its Cause Analysis. Tsinghua University Journal (Philosophy and Social Sciences Edition) ,32(05):172-182+199.

[2] Meiying Chen, Jiao Zhang. (2017). New Development of International Regulation-Formulation in Cross-border Data Flow: Dilemma and the Way Forward. Shanghai University of International Business and Economics Journal. ,24(06):37-52.

[3] Shekou WU. (2016). Studies on Transnational Data Flow and Data Sovereignty. Journal of Shanghai University of International Business and Economics,37(05):112-119.

[4] Chen, Y., & Xu, J. (2020). Cross-border data flow governance: China's perspective. International Journal of Information Management, 50, 282-288.

[5] Zhang, S., & Chen, H. (2019). The global governance of cross-border data flows: Challenges and opportunities. Journal of International Management, 25(2), 100676.

[6] The State Council of the People's Republic of China. (2023). Institutional Reform Plan of the State Council of the People's Republic of China (2023). Retrieved from http://english.gov.cn/news/topnews/202303/07/content_WS62203338c6d0df57f98b32c1.html

[7] The Central Committee of the Communist Party of China. (2022). Full text of the Resolution of the 20th CPC National Congress. Xinhua News Agency.