Journal of Computing and Electronic Information Management
ISSN: 2413-1660 | Vol. 10, No. 1, 2023

Research and Improvement of China's Data Exit Supervision Rules

Yurong Ren*

School of trade negotiations, Shanghai University of International Business and Economics, Shanghai, China
* **Corresponding author**: Email: ryrsingforu@163.com

Abstract: With the vigorous development of the digital economy, data security has created new demands on the system. Administrative punishment cases against data security such as the "Didi case" have exposed China's current shortcomings in regulating data export; In the international context, developed countries are trying to establish rules for cross-border data transfers. Under the background of both international and domestic reality, China's data export rules are constantly improving, responding to data security needs internally, and establishing a voice in rules related to cross-border data circulation externally. At present, China's legislation on data export has begun to take shape, and the operability has been significantly enhanced, but there are still legislative shortcomings such as unclear data classification standards.

Keywords: Data export; Hierarchical classification; Security assessment.

1. Introduction

In 2021, Didi wanted the SEC to file an IPO prospectus and start preparations for listing in the United States. Netizens pointed out that Didi submitted user data and map data to the coal house for listing in the United States, which seriously endangered national security and the privacy of Chinese citizens. In the case of Didi Chuxing, fines were imposed for two types of behavior: collecting user information and data in violation of the law, and failing to conduct the necessary cybersecurity checks before the data went offshore. However, when Didi was required to conduct a cybersecurity review, it was mainly conducted in accordance with the Special Provisions on the Overseas Offering and Listing of Joint Stock Companies, which requires companies to notify and obtain approval from the competent securities authorities for their overseas listings. DDT's overseas listing is known as the "first cybersecurity review" because it only conducts a cybersecurity review based on this rule, and according to other relevant regulations, Didi is a critical infrastructure facility operator and should review the impact of products and services on national security risks in accordance with the review measures. Although Didi executives did not transmit the above key information abroad, the company has been successfully listed in the United States, so it is impossible to determine whether there is really a transmission. However, as a result, Didi skipped the review link and successfully listed in the United States, to a certain extent, indicating that there were still big loopholes in the supervision of data export at that time.

2. Overview of China's data export rules

To strengthen the review of outbound information and protect the public interest and national security, since 2017, China has successively formulated and promulgated the Cybersecurity Law, the Data Security Law and the Personal Information Protection Law, and data supervision has a legal basis. The regulatory rules for data export are also based on these three laws, forming a data export supervision system with "classification and grading" and "security assessment" as the two main measures. In addition to the above three laws and safeguard measures for data export, the rules on cross-border data transfer are scattered among governance rules applicable to specific sectors and data types, such as the Regulations on the Administration of the Credit Reporting Industry and the Measures for the Administration of Population Health Information. On October 29, 2021, the Cyberspace Administration of China (CAC) issued the Measures for Security Assessment of Data Exports (Draft for Comments), which was officially released in July 2022 (hereinafter referred to as the Measures) after extensive solicitation of opinions from all parties in the society. Prior to this, the Cyberspace Administration of China issued the Measures for Security Assessment of the Overseas Transmission of Personal Information and Important Data (Draft for Comments) and the Measures for Security Assessment of Personal Information Exported Abroad (Draft for Comments) in 2017 and 2019, respectively.

According to the Measures, the key assessment content of the self-assessment before data export is closely related to the legislative objectives of data-related laws and regulations: the first assessment is the legality, legitimacy and necessity of the basic elements of data export, that is, the purpose, scope and method of data export, reflecting China's cautious attitude towards outbound data, requiring data processors to exit the country only when it meets the "legal, legitimate and necessary" requirements, rather than leaving the country without restrictions; Secondly, whether the nature of the exported data is close to "important data", and finally the security situation after the data is exported is evaluated from many aspects, not only whether the legal documents drawn up with the overseas recipient stipulate sufficient data protection obligations and the recipient's ability to perform and ensure data security, but also assess the security situation after the data is exported.

In terms of procedures, the processor of data export needs to form a sub-assessment report after completing the assessment, and shall file with the overseas recipient, wherein if personal information is exported, it shall be in accordance with the relevant provisions of the standard contract for the

export of personal information formulated by the Cyberspace Administration of China. The declaration to the internet information department will go through provincial and national assessments, the provincial internet information department will focus on checking the "completeness" of the declared materials, and the state internet information department will determine whether to accept the complete declaration materials within 7 days of receiving the complete declaration materials and notify the declarant in writing. The State departments in charge of internet information shall organize relevant departments of the State Council, provincial-level departments for internet information, and specialized agencies to conduct security assessments based on the scope of the declared data. In addition, it emphasizes the assessment of national or provincial data security protection policies and legislation of overseas recipients and the cybersecurity environment outsourced to data security marketing, as well as the level of data protection of overseas recipients, and whether the level of data protection of overseas recipients meets the requirements of laws, administrative regulations and national minimum standards of the People's Republic of China. If the assessment results are positive, the data handler may, after receiving a written notice from the Ministry of Cybersecurity, conduct data export activities in strict accordance with the Measures; Otherwise, the declared data export activities must be stopped immediately.

3. Legal analysis of China's data export system

3.1. Vague data classification rule standards

In terms of data classification, before the promulgation of the above three laws, the classification of data basically showed a trend of departmental law differentiation by industry, and the academic research on data classification showed a strong trend of departmental law differentiation, scholars in the field of private law focused on discussing the legal positioning, ownership relationship and protection path of data in private law, while scholars in the field of public law focused on the opening and governance of government data. Data grading puts forward key protected data types such as "core data and important data" and "personal sensitive information" in the field of personal information, but there is currently no formal data catalog or identification method for important data, and only the "Network Data Security Management Regulations (Draft for Comments)" issued by the Cyberspace Administration of China (CAC) clarifies its connotation, and lists seven categories of data that may be involved, but the expression of data classification is very broad and the boundaries are vague. Therefore, the descriptive definition of harm to national security and economic operation after the use of important data and core data is destroyed may lead to the generalization of the scope of data export involved in the security assessment to a certain extent, and the opacity of the security assessment standards may be caused by the different concepts held by the assessors in the implementation process.

3.2. The dilemma of personal data export

The system for the transfer of personal information abroad is more complicated. The PIPL sets a threshold for obtaining the separate consent of the information subject for the export of personal information; And the latest "Standard Contract for the Overseas Export of Personal Information". Combined with other provisions on the export of personal information, China is very cautious in its legislative attitude towards the export of personal information. Moreover, China's personal information export system is partially affected by the GDPR, taking into account the public interest, corporate interests and personal privacy protection. The export of a certain amount of personal data falls within the scope of supervision of security assessment, reflecting China's value orientation of paying attention to public interests and preventing public risks in legislation, but at the same time setting the consent of individuals as a prerequisite, that is, adding the legal obligation of enterprises to protect personal information. However, the implementation rules for personal information protection certification have not yet been issued. The real business community has analyzed the compliance of enterprises in the export of personal information: personal information protection certification is applicable to personal information transfer within affiliated companies or multinational companies, standard contracts are applicable and security assessment mandatory declaration of personal information is not the case of overseas personal information export.

3.3. Security assessment measures need to be improved

In the context of China's prevention of security risks and advocacy of national security and social public interests, data security assessment methods have emerged. The Measures clarify the scope and process of security assessment, so that there is a unified basis for the supervision of data export, which is a measure to ensure data security and will also limit the tendency of generalization of security measures.

First, the security assessment better copes with the risk characteristics under data flow and comprehensively assesses the risk of data export. The high flow of data and its easy availability makes it more difficult to regulate data unlike other market practices. However, after entering the era of big data, the harmful consequences of data destruction to different subjects will also be amplified, and the guarantee of data security cannot be limited to the data itself, and achieving risk resolution and precaution in the whole process is an important measure in this context. Therefore, the measures of comprehensive data export security assessment require that the security risks involved in data export are more comprehensive and comprehensive.

Secondly, the focus of data output security assessment is dynamic data risk prevention. Data export security assessmentIn order to ensure the security of the entire data export process, a security assessment must be carried out as a pre-existing security assessment. After passing the security assessment, the data is under the effective control of the overseas recipient, how to ensure the security of the data safely and adequately, especially when the legislation on data security and personal data protection in the country or region of the overseas recipient is different from that in order to ensure that the data is kept within the controlled range, it is necessary to sign actual agreements and other legal documents with the overseas beneficiaries and ensure that these agreements and legal documents are fully implemented.

Finally, the security assessment of data export is an assertion of China's data security sovereignty. First, in terms of cross-border data legislation, China takes the theoretical basis of data security sovereignty, and can note from the data

export security assessment and its superior law that the overall data export security assessment focuses on collective interests such as social public interests and national security. Second, in the matters of data security assessment, the data protection level of the data recipient is not lower than that of China, reflecting some data defense colors. This kind of defensibility is also the goal of the security assessment after data is exported abroad, once again proving that the security assessment is the goal of risk prevention in the whole process of data activities. From the perspective of international cooperation, the adequate assessment mechanism implemented by the EU is not only a way to prevent data risks, but also sets a threshold for its selection of partners. Therefore, this content may also become one of the important measures for data exchange between China and other countries that can cooperate.

4. The improvement of China's data export supervision rules

In the face of the ever-changing institutional needs of the digital era and the new situation of international digital trade, there is still more room for improvement in the rules for data export in China, improve the scientific nature of legislation, and take into account the legal value of data security and free circulation; Externally, we should also put forward rules and propositions with a clearer position.

4.1. Establish data grading rules

Judging from the trend of international cross-border data flow, the United States, Europe and Japan are developing new trade rules between developed countries and promoting the establishment of low-restricted, high-liquidity international cross-border data flows, while the European Union is also seeking to strengthen cooperation on cross-border data flows. At the same time, developed countries, represented by the United States and its allies, are deliberately isolating and obstructing China's participation in the process of formulating international trade rules. This trend has made it more obvious and urgent for China to improve and improve the rules of data flow.

The rapid development of the Internet and the innovation of big data have given the concept of security a new form in the digital age. The existence of big data expands the negative spillover effect after data destruction, and the risk of data destruction extends from the data itself to the whole link of processing data, which also puts forward higher requirements for data supervision measures, but if the risk prevention of the whole process of data flow is easy to ignore the benefits and value generated by data in circulation, restrict the economic benefits of data, and also make regulatory measures bear too heavy economic costs. Therefore, the control of data export needs to take into account the dual goals of data security and economic benefits.

First, from the concept of classification, China can learn from the practice of the European Union, which promulgated the EU Regulation on the Free Flow of Non-personal Data in May 2019, which basically establishes two categories: "personal data" and "non-personal data", and this classification is relatively comprehensive from a conceptual point of view. Second, after clarifying the legal concept, it should be improved in regulatory measures. Some scholars believe that at present, China's data classification is classified from the information it contains, and the personal data and public data directed to protect individuals and public interests are classified by their subjects, and "commercial data" with legal persons as the theme should be added. Based on "de-identification technology", personal data and important data can be separated from enterprise data. With reference to the provisions of the PIPL, the law expressly excludes anonymized information. It can be considered that this is the legal recognition of the "de-identified data" norm. However, there is still a lack of corresponding industry regulation and standard recognition for data containing other information. Accordingly, the flow of personal data and public data has been restricted by attaching restrictions and security assessments, so the scope of unrestricted commercial data should be added. Finally, attention should be paid to the uniformity of data export legislation. At present, many provinces and cities have issued their own regulations on data export to control data export activities, which may cause different standards and cause a burden on trade; Moreover, the connection between new and old laws and regulations, such as how to connect existing industry supervision with newly promulgated data management measures, is also one of the issues that future legislation should solve.

4.2. Drive international cooperation on data export reviews and technical standards

From the specific path of data export, although China has just promulgated standard contract clauses; However, in the absence of binding group enterprise rules, the approved certification mechanism, that is, the implementer and recipient of data export, should accept the certification of its data security technology and management guarantee capability level by the government or its accredited assessment agency, and cross-border data exchange between certified enterprises can be carried out. Moreover, the standard contractual clauses are not one of the alternative paths to exempt the security assessment of data export, but are conditions to be superimposed. In order to improve the speed of data export and create convenient conditions for data export, international cooperation at the technical level can be sought.

4.3. Actively promote the negotiation of rules for cross-border data flow in free trade agreements

As data-driven socio-economic development becomes increasingly important, facilitating the flow of data has become an integral part of the era of big data. In addition to the CPTPP, the United States, Singapore, Japan, Australia and New Zealand have signed the Digital Trade Agreement (DEPA), and a separate digital trade agreement is gradually becoming a new option in the context of digital trade. At a time when new rules and new international trade have not yet been finalized, it is important to grasp the right to speak on rules and strengthen the export of rules to participate in the formulation of international rules. As the world's second largest digital economy, China should take the initiative to participate in the international digital trade rule-making process, put forward its own suggestions, and become a leader in digital trade.

Cross-border data flow is an emerging area that China needs to step up to include in the ranks of digital trade liberalization. In the negotiation process of digital trade rules such as cross-border data flow, Singapore has mature experience in digital trade rules, such as the Digital Economy

Partnership Agreement with New Zealand and Chile will come into force in 2021, China and Singapore have signed free trade agreements, Singapore has also signed RCEP and other free trade agreements, China and Singapore have a greater chance to become the first country to successfully cooperate. China should adhere to the position of safeguarding the free flow of digital security in accordance with its national conditions and promote the formulation of rules that are in line with China's national conditions and the interests of digital trade on this position. According to the 2021 Global Digital Trade and China Development Report, China's digital economy is developing rapidly and has become one of the world's top ten digital trade economies, which is not only a source of massive data, but also a major source of overseas digital trade and investment. Therefore, China needs to understand the security red lines, balance development principles, and benefit from the free cross-border flow of data, while paying close attention to data security. In the face of increasingly fierce competition in the development of the digital economy, it is ultimately necessary to seek multi-party cooperation. How to achieve a balance between digital security and free circulation is a double test for China's system construction and international trade cooperation. The improvement of domestic technology and legislation is positive for foreign negotiations, reducing unnecessary obstacles to cross-border digital flow, amplifying the development effect brought by digital flow, and opening up a future for China to reach more cooperation.

References

[1] Susannah Hodson, applying WTO and FTA disciplines to Data localization measures, published online by Cambridge university press,vol03,2018

[2] ABE Yoshinori, Data Localization Measures and International Economic Law: How Do WTO and TPP/CPTPP Disciplines Apply to These Measures, policy research institute, ministry of finance, vol 16, 2021

[3] Anupam Chander, is data localization a solution for Schrems II? journal of international economic law, vol23, 2020

[4] LIU Jin Rui. Data Security Paradigm Innovation and Its Legislative Development [J]. Global Law Review, 2021, 43(1):3-21.

[5] XU Ke. Freedom and Security: China's Scheme for Cross-border Data Flow[J]. Global Law Review,2022,43(1):23-37.

[6] Andrew D. Mitchell, Jarrod Hepburn, Don't Fence Me in: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer, Vol.19 Yale Journal of Law and Technology182,p.191(2018)

[7] Bortnick Jane, International information flow: the developing world perspective ,Vol.14 Cornell international law Journal333, p.342(1981).

[8] G. Russell Pipe，International Information Policy: Evolution of Transborder Data Flow Issues， Vol.01 Telematics and Informatics 409, p.409(1984).

[9] HONG Yan Qing. China's Scheme for Promoting Cross-border Data Flow of the "Belt and Road": An Unfolding in the Context of the US-EU Paradigm [J]. China Law Review, 2021(02):30-42.

[10] Lee Jae Min, National Security Exception’s Untested Terrain-Scope and Problems of a ‘Refusal to Furnish Information’ Clause-, Korean Journal of International Law, Vol. 65, No. 1 (2020), pp.137-138.

[11] JOSHUA D. B.Reading the trade tea leaves：a comparative analysis of potential United States WTO-GATS claims against privacy[J].Localization and cybersecurity laws，2018，49（2）：801-843.

[12] MELTZE R J. The internet，cross-border data flows and international trade[J]. Asia & The Pacific Policy Studies，2015(1) : 90-102.

[13] ZHAO Jing Wu. Construction Foundation and Regulatory Transformation of Standardized Contracts in Cross-border Data Transmission [J]. Journal of Northwest University of Political Science and Law,2022,40(2):148-161.