ISSN: 2710-0170

Analysis on the legal problems of data exit

Zhongsen Zhang

College of Political Science and Law, University of Jinan, Jinan 250024, China

Abstract

Faced with the exponential growth of cross-border data flow, it is too weak to supervise through existing laws, regulations and rules, and the regulatory rules for cross-border data flow should be further refined and improved. This paper summarizes the existing legal problems by analyzing the current status of data exit legal supervision in our country. Based on China's national conditions and respecting the objective laws of the development of the digital economy, targeted countermeasures and suggestions are proposed from many aspects, a scientific and coordinated regulatory system for cross-border data flow is built, a dynamic balance between development and security is sought, and cross-border data governance is adapted to the growth needs of the digital economy, so as to ultimately achieve a good law and good governance for cross-border data supervision.

Keywords

Data exit, Supervision, Data sovereignty, Data governance, Cross-border data flow.

1. The main problems of China's data exit

China started relatively late in the legal regulation of data exit. However, in recent years, it has shown a rapid growth of jointing. In the previous article, we have clarified the concept of data and information. As for the legislative process of China's data exit regulation, the author temporarily divides the node into three troika of data supervision framework, and combs the legislative process of China's data exit legal regulation. Before the promulgation of the Cybersecurity Law, China's understanding of data protection and data flow adopted the regulatory approach of "who needs who makes", which made the problem of data protection and data flow appear relatively fragmented and fragmented at the legislative level. The specific norms are more scattered in multiple laws and regulations and span many disciplines such as criminal, civil and administrative. Some scholars call this kind of regulation as "patch" legislation[1].

The disadvantages brought by this mode are very obvious. The lack of specific legal provisions makes the scope of regulatory scenarios small and the actual scope of regulation narrow. Meanwhile, at the legislative level, due to the absence of specialized laws to guide, most of the provisions do not have the mandatory binding effect in law, and it is difficult to deter illegal acts. It can only be dispersed in key areas such as finance, biology, and transportation. The whole situation presents the form of "separation of all laws".

1.1. The examination method is single

In general, supervision refers to the subject's regulation of activities through specific systems and laws. The traditional mode of regulation is divided into government regulation and self-regulation. At present, in the field of cross-border data flow, the government has expressed its determination to strictly regulate by continuously promoting legislation, and self-regulation refers to the regulation of enterprises, industries and other subjects as the main body to formulate management methods. When it comes to the supervision in the field of data exit, facing the rapidly changing background of data governance, China's main foothold is from

ISSN: 2710-0170

government supervision, and market self-supervision is a means to correct and improve the inherent problems. However, since data involves national security, corporate efficiency, personal privacy and other special risks, whether it is for the protection of private entities or the maintenance of public interests, it is bound to need to carry out multi-level and multi-angle supervision as a starting point. Although the industry self-discipline has been promoted, it is still insufficient. However, some of the laws used in the current government supervision are insufficient in the construction of the compliance system. It is difficult to apply such decentralized, macro rules to real-world cases in the rapidly changing digital economy[2].

1.2. The safety review evaluation rules are not detailed

At present, the establishment of rules for data exit security review in China stays more at the macro level, so the "national security review" in the "Network Security Law" and "Data Security Law" has become the pre-procedure for data legal exit. The review methods currently based mainly refer to the "Network Security Review Measures" officially implemented on February 15, 2022, while the relevant rules for the field of data exit, "Data Exit Security Assessment Measures (Draft for comments)," have not yet landed after soliciting opinions from the public at the end of 2021. According to the current regulations, only after passing the data security review, the enterprise will be issued administrative permission to allow the exit. Although we support the concept of national security as a priority, for data countries like our country, the "first review and then exit" model is bound to consider at least two aspects of the problem. The first is the cost of the review body's work[3]. Whether it is network security review or data exit assessment, it is organized by the relevant office and collaborates with multiple departments to carry out the review and evaluation. At present, the cross-border flow of data is naturally increasing. In the era of digital economic globalization, outbound data is bound to show a continuous upward trend. This will undoubtedly increase the time cost and human resources cost for the review and evaluation subjects. Secondly, the review and evaluation body is led by one department and carried out jointly by multiple departments. Will the decentralization of power in the review and evaluation process affect the efficiency and promote the reasonable health evaluation results?

1.3. Insufficient international cooperation

In today's world, peaceful development and win-win cooperation have become the trend of The Times. Promoting development through cooperation and safeguarding peace is the guarantee of security. International cooperation and exchange have greatly alleviated the situation of insufficient data outbound resources in China, improved the state of national resources, improved the ability and quality of cooperative project management, and promoted the training of talents and the smooth development of key work in our country. In terms of cooperation with regional international organizations, developed countries in Europe and the United States involve provisions on national security review rules for data exit in bilateral and changeable trade agreements to protect the development of digital economy and trade and even protect the country.

Be safe. However, in international trade, China mainly relies on domestic laws and some unilateral trade agreements, and has not established long-term effective cooperation mechanisms with other countries or regional organizations[4].

2. The improvement of China's data exit legal regulations

Since the 20th National Congress of the Communist Party of China, network security and data security have been elevated to an unprecedented height as the foundation of cyber power and digital China. The cross-border flow of data involves not only cross-border trade, but also non-economic concerns such as national security, data sovereignty and protection of private rights.

ISSN: 2710-0170

According to the theory of data sovereignty, China has the right to supervise the cross-border flow of data and the obligation to protect data security. The European Union, the United States and other developed economies have adopted strict and comprehensive regulatory legislation. Therefore, it is imperative to improve the supervision of cross-border data flow in China.

2.1. Formulating classification and grading standards

The data has a certain crossover property. For different data content, regulators are making different restrictions and rules. In recent years, China has been advocating and calling for data classification management, data classification and classification has gradually become the main measure of data security governance[5]. Some regions and industries have also actively responded to classification and formulated a series of relevant systems. The "Personal Information Protection Law" has been implemented, personal information has been defined in detail, and important data has also been scientifically defined in the "Data Security Management Measures". The distribution of important data includes but is not limited to government agencies, enterprises in key industries, social public service institutions, scientific research institutions, etc. However, in the identification, if the extension of important data is too extended, it is easy to affect the situation of data exit, so the definition of important data has been identified standards should be combined with the real situation of the industry. Focus on national security and public interest, grasp its possible risk dynamics. According to the nature of data, the field of application, the subject of generation and reception, the concept of important data is determined, and it is classified and classified management. The hierarchical types of data should not be divided into too many details, nor should they be too rough to achieve the original idea and effect. It is necessary to improve the classification and classification of data based on its characteristics, producers, objects, exit types, and possible risks[6].

2.2. Encourage the use of standard contract terms

At present, China's Personal Information Protection Law and Network Data Security Management Regulations (draft for comment) both refer to standard contracts and regard the personal information protection certification of data processors and data recipients through professional institutions identified by the national network information Department as one of the four preconditions for data exit.

For the formulation of "standard contract terms", first, we should fully expand the scope of security assessment, and introduce more flexible binding company guidelines, codes of conduct, and authentication mechanisms in the way of data exit, so that contract compliance is no longer the only option for the parties; According to the "2021 Data Security Industry Research Report", 59.6% of the surveyed enterprises believe that the biggest challenge facing data security construction is from the lack of understanding of regulatory requirements. This shows that China still has a long way to go in the implementation of data supervision requirements. For most enterprises with data exit needs, among the four preconditions for data exit, compared with security assessment and certification by professional organizations, standard contracts are more convenient and guiding, and closer to the atmosphere of enterprises. One is because the standard contract formulated by the professional department can achieve greater protection of outbound data, and the other is because it is more efficient. In addition, it is necessary to make sure that the standard contract text is only a part of the personal information exit contract, and the personal information processor can sign more specific contracts with the overseas recipient on the rights and obligations according to its own needs. For different industries, different versions of the standard contract clauses can be drafted. As long as the provisions of the standard contract text are not modified, the protection level in the standard contract shall not be impaired. The addition of clauses shall not contradict the standard contract text and shall be allowed[7].

ISSN: 2710-0170

2.3. Appropriate delegation of assessment power

The implementation of regulatory functions is related to whether the interests can be guaranteed, whether the market can be corrected, and whether the economy can develop healthily. The data exit process involves many aspects, according to the provisions of the "Network Security Law" and "Data exit Security Assessment Measures (draft for comments)", the Network Information Office, the Ministry of Industry and Information Technology, the public security department, and the industry supervisor have supervisory powers during the exit process. China's regulatory management belongs to the centralized supervision system of the industry, that is, the multi-head audit mechanism, which is dominated by the competent industry authorities for the supervision and related review of data flow. In practical application, this kind of multi-head supervision is easy to form a situation of "anyone can manage and no one cares". The author suggests that data exit supervision and evaluation should be established by industry[8].

Special organization, set up special posts, from the supervision responsibilities, industry characteristics, safety assessment priorities and other dimensions of training staff, in the process of supervision and assessment to complete the coordination of the multi-head audit mechanism process, deal with the industry and Various matters related to data protection, in order to effectively implement various regulatory issues in the process of data exit. The identification of regulators is not inconsistent with the centralization and appropriate decentralization of assessment powers[9].

2.4. Participating in international rule-making

Although the European Union, the United States and other international organizations, developed countries have formulated relevant rules on cross-border data flows, but there is no uniform international rules or treaties on a global scale[10]. In view of this, China should actively participate in regional cooperation organizations and participate in the formulation of national security assessment rules for data exit in order to protect China's legitimate rights and interests in data. Specifically, China should seize the historical opportunity, actively participate in the study of cross-border data flow, put forward their own proposals, introduce China's data exit standards, protect China's data legitimate rights and interests, and promote international exchanges and the prosperity of international economic trade. Actively participate in the formulation of global data rules, add provisions on cross-border data flow in the current bilateral and multilateral trade negotiations, and lay the foundation for Chinese digital enterprises to "go global"[11]. Efforts will be made to promote the formulation of data flow agreements and standards under the "Belt and Road" cooperation framework, build a community of shared future in digital space, and promote the formation of a new situation in the regulation of global cross-border data flow. In specific practice, we should actively fulfill international obligations and assume international responsibilities, and take relevant measures to effectively respond to overseas countries that have unfair treatment or discriminatory measures against China's data trade, so as to safeguard our national security and ensure the development of our international trade[12].

3. Conclusion

As a country with a huge volume and still in the process of development, China emphasizes data sovereignty and national security. However, with the requirements of the 14th Five-Year Plan and the establishment of the "double cycle" pattern, our country increasingly encourages the idea of attaching equal importance to security and development. Although China has initially established a legal framework for cross-border data flow, in the actual operation, a more relaxed environment should be given to reasonable outbound demand. We can learn from the

ISSN: 2710-0170

European and American models, increase outbound channels by classifying data, formulating outbound data whitelist, carrying out standard contract terms, and introduce autonomous self-examination of industries and enterprises. Improve their own management level, in terms of hardware supporting, support the development of data technology, do a good job of science and technology to support legal regulations, and improve China's supervision and regulation of data exit. Use regional organizations to promote the establishment of bilateral or multilateral data cross-border flow rules, put forward China's plan, give play to the status of data power, promote the international basic rules of data cross-border flow, and enhance China's voice in data governance.

References

[1] Tan Guanfu. International Law regulation of cross-border data flow in digital trade [J]. Comparative Law Studies,2022,(03):169-185.

[2] [Zhang Guang, Song Ge. Global rule game and China's path selection under Digital economy: from the perspective of cross-border data flow regulation.] Academic Exchange,2022,(01):96-113+192.

[3] Haibin Chen, Noah Wang. Research on cross-border data flow governance in Japan [J]. Information Theory and Practice, 2019,44(12):197-204. (in Chinese)

[4] Ma Qijia, Li Xiaonan. Research on regulatory rules of cross-border data flow in the context of international digital trade [J]. International Trade,2021,(03):74-81.

[5] Game and cooperation of cross-border data flow rules in Europe, America and Japan. International Trade,2021,(02):82-88.]

[6] Ma Qijia, Li Xiaonan. On the construction of regulatory rules for cross-border data flow in China [J]. Rule of Law Research,2021,(01):91-101.

[7] Zeng Yuemei. Research on Legal Regulation of cross-border Data Flow [D]. Guangxi University,2020.

[8] Wu Shenkuo, Zhang Liwei. System design and countermeasures of a new agreement on cross-border data enforcement in the United Kingdom and the United States [J]. China Information Security,2019,(12):60-63.

[9] Zhang Duan. On Public interest Protection of cross-border Data Flow [J]. Hebei Law School, 2018, 36(05):180-190.

[10] Wang Gongzheng. On the rule of Law process of China's network domain normative governance -- from the perspective of the evolution of the Network Security Law [J]. Journal of Xidian University (Social Science Edition),2017,27(04):73-83.

[11] Huang Ning. Research on the impact and policy motivation of data localization. China Science and Technology Forum,2017,(09):161-168.

[12] Gao Fuping, Wang Yuan. Legal Obstacles to the transplantation of the Right to be Forgotten in China: A case study of Ren Jiayu and Baidu [J]. Application of Law (Judicial Cases),2017,(16):40-47.