VNU Journal of Science: Legal Studies, Vol. 38, No. 1 (2022) 36-50

VNU Journal of Science: Legal Studies

Journal homepage: https://js.vnu.edu.vn/LS

Original Article

Analysis of Data Exit Security Review under the Background of Digital Trade: with Comments on the Chinese Measures for Data Exit Security Assessment (Draft for comments)

Zhang Liying*, Duan Jiabao

School of International Law, China University of Political Science and Law

Received 15 March 2021
Revised 20 March 2021; Accepted 26 March 2021

Abstract: Data exit brings new growth and opportunities for the development of digital trade in various countries, but without regulation, it may damage national security interests. Therefore, it is necessary to study the review rules of data exit, which is of great significance to maintain national security and ensure the development of digital trade. Therefore, under the legal basis provided by the Cybersecurity Law and the Data Security Law, China actively explored and formulated specific rules for data exit assessment, and published the Measures for Data Exit Security Assessment (Draft for comments) (hereinafter "the Measures") in October 2021. The Measures is undoubtedly a beneficial attempt to protect national security and realize the orderly exit of data. It has made a significant breakthrough in relevant rules. However, there are still some rules to be improved. In terms of such rules in other territories, the United States and the European Union have adopted data exit review mechanisms with different value orientations, which have their own advantages and characteristics, can provide references for China to improve data exit security review rules.

Keywords: Data exit, national security, digital trade.

1. Introduction

In the digital trade era, a large number of enterprises going abroad for listing will inevitably involve data going abroad. The issue of China concept stock data caused by Didi's listing in the United States has attracted public attention. On June 30th, 2021, Didi was listed in the United States, but there was no press conference or bell-ringing ceremony. The reason is that Didi's listing in the United States did not obtain the prior consent of the Chinese

* Corresponding author.
E-mail address: djb0103@163.com
https://doi.org/10.25073/2588-1167/vnuls.4429

regulatory authorities, that is to say Didi's listing bypassed the regulatory authorities. Didi's listing can bypass the regulatory authorities because it adopts the "small red chip" mode, which means that domestic natural persons establish holding companies overseas (controlled by domestic natural persons) and turn domestic operating entities into subsidiaries of overseas holding companies or variable interest entities (VIE), then finance or complete listing through overseas holding companies. As the listed entity is registered overseas, the CSRC has not set up relevant domestic pre-approval procedures at present. However, although Didi has escaped the regulation of the securities law, it has not escaped the relevant regulation of network and data security. On July 2nd, China Cybersecurity Review Office (hereinafter "the Review Office") issued an announcement to implement Cybersecurity review on "Didi travel". During the review period, Didi travel stopped registering new users. Then, the State Internet Information Office (hereinafter "the Office") informed the App store to take off the "Didi travel" App and rectify the serious illegal collection and use of personal information. Faced with the heavy blow of the falling share price, Didi announced its delisting in the United States on December 3rd. Didi has mastered a large number of underlying data related to national infrastructure construction and national development. This security review reflects that China not only protects personal information security, but also attaches importance to national information security, and the complexity of the environment in data exit amplifies the threat to national information security. Although the security review of Didi is based on the measures for Cybersecurity review, the exit security of data will be more involved in the issue of enterprise listing. However, there is a lack of data exit management regulation in China. Therefore, under the legal basis provided by the Cybersecurity Law and the Data Security Law, China has promulgated the Measures in October 2021 to specifically standardize the security assessment of data exit. However, the assessment method is still in the stage of soliciting opinions, and its relevant rules need to be further clarified and improved. In terms of the relevant rules of data exit security review, the legislative practice of the EU and the United States can be used for reference. This paper will discuss the legislative breakthrough of the Measures, analyze and point out its limitations, and put forward suggestions on the improvement of China's relevant rules in combination with the research on those rules in EU and the U.S.

2. The Developing Needs of Data Exit and its Challenges to National Security

The exit of data is related to the dynamic balance between national interests and the development of the digital economy. On the one hand, loose data cross-border flow rules are conducive to the development of industrial digitization. However, it will increase the difficulty of risk control, which may damage the national interests of a country, especially developing countries. While for developed countries, it will help them implement global economic control through data. On the other hand, strict cross-border data flow rules are not conducive to the development of industrial digitization, but will reduce the difficulty of risk control. For developing countries, it can avoid the data hegemony of developed countries to a certain extent.

2.1. Data Exit is an Inevitable Choice for the Development of Digital Trade

Data exit is an inevitable choice to promote the in-depth development of a digital economy. In economic and trade cooperation, it is necessary to optimize the allocation of resources through big data. The application of digital technologies such as big data is conducive to accelerating the emergence of some new business forms, new models and new industries. To be more specific, there are four reasons to explain why data exit is so important and inevitable for the development of digital trade.

First, the cross-border flow of data has

greatly promoted economic development. Cross border data flow not only supports the globalization activities of almost all other elements, including goods, services, capital and talents, but also plays an increasingly independent and important role. Cisco's data analysis shows that during 2015-2024, the potential minimum value of cross-border flows (defined as the dual meaning of increasing revenue and reducing costs, which is generated and transferred between companies and industries due to the adoption of Internet technology) is estimated to be $29.7 trillion [1]. It can be seen that the cross-border flow of data will improve the overall effectiveness of the whole social economy, which is of great positive significance to the economic growth of countries and enterprises.

Second, the cross-border flow of data is an important catalyst for national innovation. According to Frost & Sullivan's 2025 general trend forecast, the data support the future, and 90% of the transformative transformation depends heavily on the data [2]. At present, almost all industries rely on the flow of cross-border data and the ability to analyze data in real-time as the driving force for their supply chain, operation and business model innovation. The cross-border flow of data makes innovative ideas spread all over the world, so that Internet users all over the world can access and make use of the latest research results and technologies, stimulate more creativity, give birth to new businesses, new models and new enterprises, and realize the overall improvement of national innovation ability.

Third, the cross-border flow of data promotes the business expansion of enterprises. The open and interconnected nature of the Internet meets the natural global business needs and convenience of enterprises. Data is the "blood" of enterprise operation. WEF Global Information Technology Report 2016 believes that it is the cross-border data transmission capacity that optimizes enterprise operation and enables enterprises to rethink their methods [3]. Taking cross-border e-commerce as an example, Alibaba, Amazon and other Internet platform enterprises obtain, process and transmit data across borders through the Internet, build a global user community for all kinds of cross-border traders, realize the global expansion of the e-commerce model and help enterprises integrate into the global supply chain. At the same time, the cross-border data flow of enterprises reduces the cost of enterprise trade and transaction, and a large number of small and medium-sized companies have almost the same international trade capacity as large enterprises.[1]

Fourth, the cross-border flow of data could protect users' digital rights.[2] Taking cloud computing as an example, according to Cisco's prediction, the global cloud data center traffic will reach 19.5zb per year by 2021, and there will be 628 super large-scale data centers in the world in 2021 [5]. The cross-border data flow model based on cloud computing weakens the constraints of geographical storage location, and users can flexibly select cloud computing service providers worldwide according to the service content, quality and cost, which can improve users' service level and experience and protect

[1] The report of the US international trade center estimates that cross-border data flow has reduced the global trade cost by an average of 26%. The survival rate of small and medium-sized enterprises trading on various global business platforms using the Internet is 54%, 30% higher than offline enterprises [4].

[2] For instance, the digital rights could include the right to personal data and the right to data property. The right to personal data, i.e., the right of a natural person to control and dispose of his or her personal data and exclude others from interfering with it in accordance with the law. By its nature, the right to personal data, although related to property interests, is not a property right, but a new type of personality right that has been gradually clarified and independent with the development of society. The right to personal data includes the right to data decision, the right to data confidentiality, the right to data inquiry, the right to data correction, the right to data blocking, the right to data deletion and the right to data remuneration request. Data property right is the right of the right holder to directly dominate specific data property and exclude others from interfering with it. It is a new type of property right born in the era of big data.

users' digital rights.

2.2. Risks to National Security Caused by Data Exit

As mentioned above, the cross-border flow of data itself is a "double-edged sword". On the one hand, it can promote the development of digital trade and further activate the global digital economy. On the other hand, it may damage national security and bring legal risks. The logic behind the threat of cross-border data flow to national security can be reflected in the way of data generation and its relationship with national security interests. Specifically, data can be divided into original data and derivative data. Raw data refers to data generated without relying on existing data, which is closely related to national security. Derived data is the data obtained by processing the original data, which can be further subdivided into statistical data and big data. Statistical data and big data are generated based on original data, but there are differences in application theories, methods and technologies [6]. The original data constituting statistical data and big data itself has no connection or weak connection with national security, but the derived data obtained after technical processing, that is, statistical data and big data, are related to national security interests.

In terms of statistical data, it mainly refers to the attribute data of each specific field. A single point can be measured or disclosed, but the centralized and batch data leakage may endanger national security, military action or counter-terrorism security [7]. Taking transportation as an example, key railway route map, station layout, track distribution, storage data and other data can be made public, but such data can be gathered together to obtain the overall transportation status information of a country through simple statistical means, which may pose a threat to national security and interests once leaving the country. In terms of big data, it is not just a simple collection of original data like statistical data, but identifies the information hidden in the original massive data through data mining, machine learning and other technologies, reflecting the content that the original data or statistical data cannot reflect or reveal [8]. For example, personal consumption data itself is not directly related to national security, but after a large number of personal consumption data are gathered abroad, a country may infer the food preferences, living habits, health status and career choice preferences of residents of other countries through data mining technology and machine learning technology, so as to form an accurate portrait of the social conditions of other countries. And then, it would carry out targeted intelligence collection, research and judgment, and may even attack the weak links of other countries' economies and society.

Therefore, the national security risks brought by cross-border data flow has attracted the attention of many countries. On August 6th, 2020, the Trump Administration banned the use of TikTok and WeChat in the United States on the grounds that they were suspected of transmitting personal data of U.S. users to the Chinese government, which may damage U.S. national security. Moreover, China's Internet enterprises face serious obstacles in overseas market access. For example, the M & A investment of Huawei and ZTE in the United States and Australia and the acquisition of American Express Gold by Ant financial services ended in failure. The overseas investment of China's digital enterprises is often rejected by the host government due to national security review. One of the reasons is that digital enterprises need to collect and generate a large amount of data in the host country, and transmit the data to the domestic processor or headquarters for analysis through the cross-border data flow. On July 16th, 2020, the European Court of Justice banned the cross-border transmission of data on the grounds that Facebook violated the privacy and security of data subjects by transmitting EU users' personal data to the United States.

In addition, under the situation of serious imbalance in the development of digital industry in countries around the world, data continues to accumulate from developing countries to

developed countries, resulting in a data gap, which may contribute to the formation of data hegemony, increase the digital economy dependence of developing countries on developed countries, and further evolve into another important weapon of unilateralism. This has caused countries, especially developing countries, to worry about their own economic security.

To sum up, in the context of digital economic globalization, data, as a key production factor in international economic and trade activities, has the realistic demand of going abroad. However, the interests or values contained in data itself are diverse and intertwined, and unrestricted data flow may damage a country's national security interests. Therefore, a country should establish a normative system to effectively regulate the exit of data.

3. Extraterritorial Practice of Data Exit Security Review

At present, the global data exit security review rules have not been formed. Developed countries and regions represented by the European Union and the United States, and developing countries represented by China have developed their own unique data flow regulation models in theory and practice. However, because the discourse power of rules often differs in the influence due to the economic strength of a country or region, at present, the two main review models are those of the United States and the EU.

3.1. The United States: the "External Loosening and Internal Tightening" Review Mode under the Concept of "Active Opening"

From the perspective of the United States, it generally adheres to the policy-making attitude that data flow should not be over-regulated. With the rapid rise of e-commerce at the end of the 20th century, the United States realized that excessive regulation of the Internet might hinder economic development. Therefore, the U.S. government balanced a series of priorities and tended to flexible and customized self-regulation [9]. However, the United States has taken more stringent measures to regulate the data flow of national security. Specifically, it mainly includes the following aspects:

First, restrict the export of important technical data and foreign investment in specific data fields. Since the Trump administration vigorously pursued the "America first" trade protectionism policy, the United States has actively used control measures as an important means to curb strategic competitors such as China. The John McCain National Defense Authorization Act (NDA) of the United States in Fiscal Year 2019 updated and reformed the U.S. measures on foreign investment review and export restrictions on emerging basic technologies.[3] In terms of export control, according to the Export Administration Regulations (hereinafter "EAR"), the export control of the United States is not limited to the export of hardware, but also includes specific technical data, that is, the controlled technical data is "transmitted" to servers located outside the United States for storage or processing, which requires an export license from the Bureau of industry and security (hereinafter "BIS") of the Ministry of Commerce [10]. In January 2018, BIS issued a list of 14 types of cutting-edge technology blockades to develop an export management system framework for key technologies and related products, including 14 core cutting-edge technologies such as biotechnology, artificial intelligence and machine learning [11]. In terms of foreign investment review, the Committee on Foreign Investment in the United States (hereinafter "CFIUS") has the right to review and restrict a wide range of investment and export transactions

[3] The main contents of NDAA include Foreign Investment Risk Review Modernization Act (FIRRMA), Export Control Reform Act (ECRA), China Investment Activity Report, and the Establishment of Artificial Intelligence National Security Committee.

when necessary, and establish a variety of mechanisms to identify and protect key emerging technologies to ensure the security of the United States.[4] The reformed Foreign Investment Risk Review Modernization Act expands the scope of "covered transactions" and includes companies involving so-called "key technologies" and "key infrastructure" and non-controlled and non-passive investments by foreigners in companies that preserve or collect sensitive personal data of U.S. citizens. At the same time, CFIUS also requires investors to sign a security agreement, which stipulates the detailed contents of the internal security management system, localization of products and services, government review power, etc., so as to prevent sensitive information, products and services from leaving the country.

Second, develop a list of controlled unclassified information (hereinafter "CUI") to define the scope of "important data". According to the requirements of executive order No. 1356 signed by the president of the United States in 2010, in order to improve the current situation that the government-controlled non-secret information stipulated in U.S. laws, regulations and government policy documents is too scattered and has no unified requirements, the U.S. archives administration takes the lead and relevant government departments cooperate to sort out and unify the classification and basis of controlled non-secret data stipulated in U.S. laws, regulations and government policies, form CUI lists. CUI lists 17 categories in detail, including agriculture, controlled technical information, key infrastructure, emergency management, export control, finance, geographic product information, information system vulnerability information, intelligence, international agreements, law enforcement, nuclear, privacy, procurement and acquisition, proprietary business information, security act information, statistics, taxation, etc. Such data can be regarded as the "important data" identified by the U.S. government, and more strict management measures are taken. At the same time, the communication scope of CUI is divided into seven categories: prohibited to foreign countries, special for federal employees, special for federal employees and contractors, not open to contractors, controlled open list, only allowed to be opened to some nationals and only displayed [12].

Third, expand the scope of extraterritorial application of domestic laws through "long arm jurisdiction" to meet the law enforcement needs of cross-border data access under the new situation. In 2018, the U.S. Congress passed the Clarifying Legal Overseas Use of Data Act (hereinafter "CLOUD Act"), ending the dispute over whether U.S. law enforcement agencies have the right to obtain user's data stored in overseas servers by U.S. enterprises in the Microsoft v. FBI case. By applying the "controller principle", the law expands the power of U.S. law enforcement agencies to access overseas data, and sets a specific path for the U.S. government to sign bilateral treaties with other countries, allowing qualified foreign government law enforcement agencies to access data stored in the United States. One of the factors considered in the identification criteria of a qualified foreign government involves showing determination and commitment to the free flow of global information and maintaining the open, distributed and interconnected nature of the Internet. In addition, the foreign government should take appropriate procedures to minimize the acquisition, retention and dissemination of information involving

[4] The proposed export management system framework for key technologies and related products announced by BIS in November 2018 includes fourteen core cutting-edge technologies, such as biotechnology, artificial intelligence and machine learning technology, positioning, navigation and timing technology, unprocessed technology, advanced computing technology, data analysis technology, quantum information and sensing technology, logistics technology, additive manufacturing, robot, brain computer interface, hypersonic aerodynamics, advanced materials, advanced monitoring technology, etc..

"Americans". The CLOUD Act intensifies the current conflict of judicial sovereignty related to data between countries. If other countries want to access data stored in the United States, they must pass the review of the "qualified foreign government" of the United States and meet the standards of human rights, the rule of law and free data flow set by the United States [13].

3.2. EU: the "Conservative and Strict" Review Mode under the Concept of "Data Sovereignty"

The review mode of cross-border data flow adopted by the EU is different from that adopted by the United States. By putting forward the concept of "digital sovereignty", the EU hopes to enhance its control over the data itself, rather than just regard the data as a subsidiary of investment, industry or technology, and strengthen the data exit review system.

In July 2020, the EU released the European Digital Sovereignty Report [14], emphasizing that "digital sovereignty" should refer to Europe's ability to act independently in the digital world, which needs to be understood as a protective mechanism and defensive tool to promote digital innovation to deal with data theft and improper value evaluation based on data. In the context of digital sovereignty, it is required that the data utilization behavior of enterprises outside the EU must comply with the values and principles of the EU, including, of course, not damaging the security interests of the EU. However, it should be made clear that national security belongs to the jurisdiction of EU Member States. It is difficult for the EU to formulate unified judgment standards on whether data exit damages national security. For example, the EU Regulation on the Free Flow of Non-personal Data [15] clearly states that EU member states can take data localization measures on the grounds of national security, but impose additional constraints on the principle of "proportionality". The GDPR stipulates the specific rules for data exit through the special chapter of Chapter V "transfer of personal data to third countries or international organizations", including the unified performance of corresponding evaluation responsibilities by the European Commission and the establishment of general exit strategies such as adequacy standards and appropriate safeguards. However, it should be noted that GDPR focuses on the protection of personal rights and interests. Its evaluation standards on the adequacy and appropriate safeguards are aimed at the personal privacy and do not actually involve the evaluation procedure of national security. Therefore, the EU has not formed a relatively unified regulatory idea and path on the national security review of data exit, which is still specified by each member state. However, its concept of "data sovereignty" undoubtedly closely combines data with national interests, including security interests [16]. It is unknown whether Member States will conduct an exit security review of data to protect national security with reference to the data exit rules set by GDPR, but this possibility cannot be completely excluded. If Member States refer to the relevant rules of GDPR, it will be a "strictly conservative" review mode. This is reflected in the following two aspects,

First, determine the “white list countries” of cross-border free flow of data through "sufficiency identification", which are not restricted by the cross-border flow of personal data of the EU. The EU's consideration of "adequacy identification" includes political factors, the rule of law factors, data protection legislation and law enforcement, international agreements signed, etc. To a certain extent, the "Sufficiency determination" rule has had a significant impact on the reform of personal data protection laws in other countries and improved the global demonstration effect of EU personal data protection rules. At present, there are 13 “white list countries” confirmed by the European Commission, including Andorra, Argentina, Canada (business organization), the United States (only limited to the privacy shield framework), etc. GDPR also allows the European Commission to determine the adequacy of a specific region, one or more sectors within a third country or international organization.

Second, provide diversified ways of the cross-border flow of personal data under the condition of observing appropriate safeguards. In the absence of sufficient identification, the EU also provides enterprises with a transfer mechanism under the condition of compliance with appropriate safeguards, including legally binding and enforceable documents between public authorities or institutions, Binding Company Rules (hereinafter "BCR"), standard data protection provisions (approved by the European Commission/approved by the regulatory authorities of Member States and recognized by the European Commission), approved code of conduct, approved certification mechanism, etc. These mechanisms provide alternative cross-border data flow mechanisms for enterprises collecting and processing personal data in the EU. Taking BCR as an example, the subjects involved include multinational corporations with their headquarters or branches in EU Member States and EU Data Protection Authority (hereinafter "DPA") as a regulator. If a multinational company plans to apply BCR, it is necessary to formulate unified personal data protection rules within the company, and then the head office or branch of the multinational company located in EU Member States shall apply for BCR approval to the EU data protection authority. The approved BCR will have an effect on the data transfer behavior of all members of the multinational company and their employees within the multinational company. However, the approval requirements of EU member states are very strict and require a long approval process. In terms of responsibility allocation, a heavier responsibility is imposed on companies established in EU Member States. If the head office and branch outside the EU violate the BCR clause, the data protection authority will require the EU enterprise representative of the multinational company to bear the responsibility for violation [17]. It can be seen that the EU still adopts a cautious and conservative attitude towards data exit.

To sum up, the United States generally adopts a loose data exit policy, but the data exit regulation involving national security is very strict, showing the characteristics of "loose outside and tight inside". As for the EU, although it has not yet involved the exit evaluation rules of national security, it is not difficult to imagine that in terms of relevant norms, it may implement "strictly conservative" data exit regulation measures with reference to the consistent style of GDPR.

4. Legislative status and discussions of data exit safety assessment in China

At present, China's cross-border data flow management system is being formulated and improved. The Cybersecurity law puts forward exit security assessment requirements for key information infrastructure data. Before that, some industry departments put forward data localization storage requirements through regulations or normative documents. On October 29th, 2021, in order to refine and implement the data exit management requirements of superior laws such as the international security law, the Cybersecurity Law and the Data Security Law, the Office issued the Measures, which comprehensively and systematically put forward the "security inspection" of China's data exit requirements. It aims to ensure the healthy and orderly development of the digital economy and deal with the security risks of cross-border data transmission and overseas convergence. The Measures has made breakthroughs in some rules, but there are still some limitations. Therefore, it is necessary to conduct a comprehensive study on it, so as to better improve China's data exit review rules.

4.1. The Breakthroughs of the Measures

Before the introduction of the Measures, China only stipulated in the Cybersecurity Law and other laws that the security assessment of key information infrastructure data should be carried out, and the specific implementation rules did not have corresponding provisions. According to Article 37 of the Cybersecurity

law, Article 31 of the Data Security law and Articles 36 and 40 of the Personal Information Protection Law, operators of key information infrastructure and personal information processors who process personal information to the amount specified by the National Network Information Department need to provide data abroad, shall pass the security assessment organized by the National Network Information Department. Although some industry departments have made provisions through regulations or normative documents, there is a lack of overall guidance and applicability because they belong to departmental normative documents. Therefore, the primary significance of the Measures is that after it takes effect, it will become a "universal" guiding norm for all industries in China, so as to comprehensively regulate China's data exit security. Moreover, in terms of specific rules, compared with previous legislation, such as the Measures for Exit Security Assessment of Personal Information and Important Data (Draft for Comments) on April 11th, 2017 and the Measures for Exit Security Assessment of Personal Information (Draft for Comments) on June 13th, 2019, the Measures have also made some breakthroughs, mainly reflected in the following points:

First, whether it is a critical information infrastructure (hereinafter "CIIO") operator or not, the exit of important data requires security assessment. Prior to the issuance of the assessment measures, the current legislation only made it clear that the important data collected and generated by CIIO in domestic operations need to be subject to security assessment before leaving the country. Article 4 of the assessment measures clearly stipulates that "exit data contains important data", whether CIIO or not, shall be subject to security assessment, thus further expanding the scope of security assessment. This change is obvious and more realistic and feasible - with the development of the digital economy, it is objectively unrealistic and unnecessary for a single administrative department to exercise the responsibility of prior supervision over all cross-border data flows. On the premise that the Data Security Law defines the data classification and grade for different levels of protection and supervision measures, this change in the Measures is not only due, but also the top priority that subsequent enterprises need to pay attention to in the actual operation process.

Second, the Measures clarifies the quantity standard of personal information processed by personal information processors who need security assessment. Before the issuance of the evaluation measures, the personal information protection law only stipulated that when a personal information processor whose personal information reaches the amount specified by the national Internet Information Department provides overseas personal information collected and generated in China, it shall conduct security evaluation, but it did not specify the "specified amount". The assessment measures further clarify that "personal information processors who process personal information up to one million people" need to conduct security assessments to provide data abroad. However, there may be special provisions in some industries. For example, several provisions on Automobile Data Security Management (Trial Implementation) stipulates that "personal information involving more than 100,000 personal information subjects" is regarded as important data. If it needs to be provided abroad, it shall pass the security assessment. Compared with the threshold of "one million", the automobile industry has set stricter restrictions on data exit. At this time, it shall be applied in accordance with the principle of "special superior to general".

Third, new restrictions on the amount of personal information provided abroad. In addition to the limit on the number of people handling personal information, the assessment measures also stipulate the amount of personal information provided abroad, and distinguish between general personal information and sensitive personal information. The Measures stipulates that "if more than 100,000 people or more sensitive personal information is provided overseas in total", a security assessment shall be conducted. It is worth noting that the threshold is

not high for large and medium-sized data processors, whether it is the number limit of personal processing information or the number limit of providing personal information externally. The network information department has relatively strict supervision on personal information processing.

Fourth, the Measures clarifies the way of data exit security assessment, and combine self-assessment with a security assessment. Article 5 of the assessment measures clearly stipulates that "before providing data abroad, data processors shall carry out data exit risk self-assessment in advance", which does not emphasize that risk self-assessment needs to be carried out in advance only when security assessment is applicable. Therefore, in theory, risk self-assessment is applicable to all data exit situations, whether it involves important data or personal information meeting certain conditions mentioned above. Articles 6, 7, 10 and 11 of the Measures stipulate the specific process of safety assessment. In order to facilitate understanding, this paper illustrates the workflow of security assessment through the following diagram.

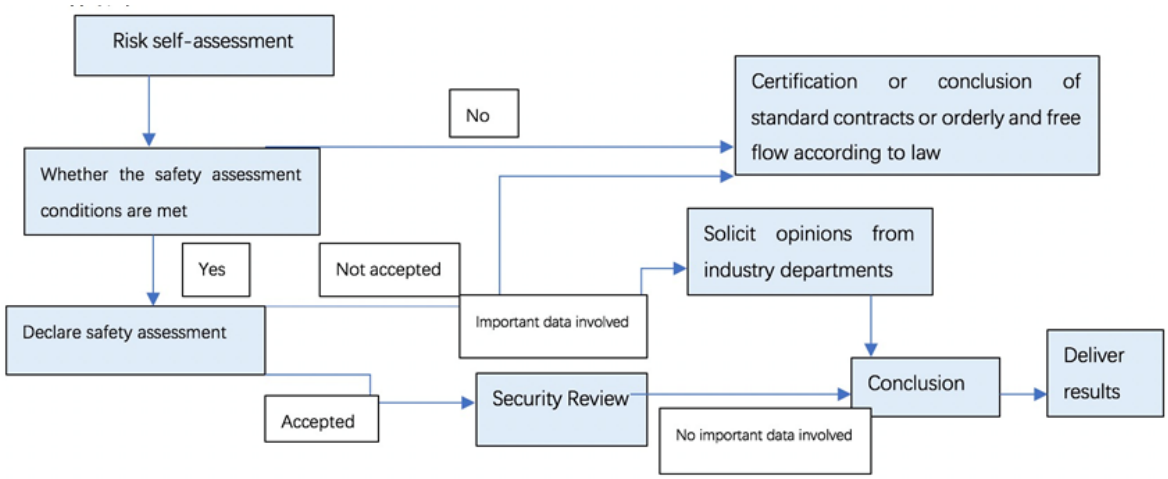

Figure 1. Review process set in the Measures.

In particular, the Measures clarify the leading position of the National Network Information Department for data exit security assessment. The "specialized agency" is mentioned for the first time in Article 10. The author believes that this agency may be a specific evaluation agency designated by the National Internet Information Department.

Fifth, the Measures emphasizes data security review. Compared with the previous measures, the Measures put more emphasis on the review of data security during and after data transfer, and the review content is more practical. For example, it strengthened "whether the management and technical measures and capabilities to fulfill responsibilities and obligations can prevent the risks of data leakage and damage", which can be proved by preparing materials, and avoided "Whether the contract can be effectively implemented" This kind of review requirement that is difficult to determine the standard. At the same time, coupled with the self-assessment of data exit risk, it is equivalent to compacting the responsibility for the exit assessment of some non-important data on the enterprise itself or the entrusted and hired third-party institutions, so as to achieve the balance between the development of data economy and administrative examination and approval by means of post-supervision. It can be seen that after the formal implementation of the Measures, whether its self-assessment or entrusting a third-party organization to assess, enterprises will inevitably add an additional part of the cost in

data exit review, but this is also the due meaning of relevant enterprises to fulfill the responsibility of data sovereignty protection.

Generally speaking, compared with the previous legislative documents, the management system established by the Measures is more mature, and has formed a good connection with the superior law and other relevant regulations on the safety management of cross-border data flow in terms of concept and system construction. With the gradual clarity of concepts and the continuous introduction of other supporting laws, regulations and policy documents, the introduction of the Measures marks an important and solid step in building a data exit security management system in China.

4.2. The Limitations of the Measures

Although the Measures has made some "achievements", it is not difficult to find that its provisions are still limited in terms of scope of use and operability, such as unclear expression and specification. The details are as follows:

Firstly, there is uncertainty in the scope of application. It mainly involves two aspects, namely "network operators" that "should apply" and "other individuals and organizations" that "refer to implementation". On the one hand, the Measures clearly point out that it is applicable to the situation that "personal information and important data collected and generated by network operators in the operation of the PRC… need to be provided overseas due to business needs". However, it is noteworthy that Article 37 of the Cybersecurity Law, as the superior law, only requires "operators of key information infrastructure" to carry out data exit security assessment on their "personal information and important data collected and generated during operation in the PRC", rather than all "network operators" and their collected relevant data. The Measures stipulate that its applicable object is "network operators", which will greatly expand the legal scope of application of the data exit security assessment mechanism under the Cybersecurity Law. This is regarded as a major breakthrough to be discussed for the existing provisions of Article 37 of the Cybersecurity Law, which is the basis of its superior law. Considering that the amount of "network operators" is already very large, and its identification is still unclear, expanding the scope of application of the evaluation measures will not only increase the legal obligations of "network operators", but also bring uncertainty to the compliance work of market operators in the network era. On the other hand, in addition to clarifying the scope of the data exit security assessment mechanism that should be applied, the Measures further pointed out that the relevant provisions of the Measures should also be "implemented by reference" for the "exit security assessment of personal information and important data collected and generated by other individuals and organizations within the territory of the PRC". The requirement of "reference implementation" will undoubtedly further expand and generalize the applicable objects of the data exit security assessment mechanism, resulting in the de facto universality and normalization of the data exit security assessment mechanism. As mentioned above, from "key information infrastructure operators" to "network operators", the scope of application of the Measures has made the first major breakthrough compared with its upper legal basis. Although it is only "reference implementation" from "network operator" to "other individuals and organizations", considering that such reference implementation in the Measures does not further limit online or offline, specific industries or fields, use purposes and situations, the author believes that it is still possible to apply it to a large number of enterprises. Different types and large-scale data processing activities carried out by individuals and other organizations cause an unnecessary burden. Therefore, the legislative and regulatory intent of the Office will need to be further clarified.

Secondly, the operability of evaluation rules is not that strong. As mentioned earlier, according to different data exit situations, the Measures basically divide the security assessment into two categories, namely self-

assessment and security assessment. In terms of security assessment, Article 9 of the Measures clearly lists the data exit situations that must be reported to the competent or regulatory authorities for security assessment, that is, network operators are obliged to report to relevant departments for security assessment only when specific conditions are met. It is worth noting that, first of all, item (5) of Article 9 is the specific situation specified in Article 37 of the Cybersecurity Law, while other situations do not appear in the provisions of the Cybersecurity Law or the National Security Law. This also shows that the Measures not only makes a breakthrough of the scope of the "subject" of data exit security assessment (the two breakthroughs mentioned above), but also the scope of the applicable "object", that is, the "data". Secondly, in all cases specified in this article, only items (i) and (ii) contain low information or data volume requirements, and other items are identified only based on the nature of the data or the subject of the implementation behavior. However, the industry scope involved in the identification standard is relatively broad, which is easy to confuse many enterprises on whether to apply for evaluation. Therefore, if it is necessary to strictly comply with the provisions of the Measures in practice, legislators may be required to clearly explain the corresponding nature of data and the scope of subjects through subsequent supporting implementation rules, so that network operators can judge the applicability of the legal evaluation mechanism, so as to enhance the operability of the legal evaluation mechanism.

Thirdly, the setting of "may affect national security and social public interests, and the industry competent or regulatory authorities think it should be evaluated" in the bottom-up clause in item (6) of this article also increases the uncertainty for the implementation and implementation to a certain extent. On the one hand, even though the National Security Law defines the concept of "national security" [18], the "social public interest" has never been clearly stipulated at the legal level. On the other hand, when the affected legal rights and interests are not completely clear, the introduction of the discretion of industry directors or regulatory authorities as one of the criteria for legal evaluation will also increase uncertainty for the unclear system construction.

Finally, the Measures also require that the statutory assessment "should be completed within 60 working-days, feedback the security assessment to the network operator in time, and report to the national network information department" (Article 10(3)). It can cause several questions, such as, whether the evaluation department will issue a written evaluation opinion on the decision to approve or disapprove the data to leave the country? Or, whether the network operator has the right to file a reconsideration without approval? If so, the series of questions such as the specific operating rules of reconsideration are practical problems that enterprises are difficult to bypass when performing the obligation of data exit security assessment, and the current Measures have not given an answer.

4.3. Reflections on China's Data Exit Review Rules under the Concept of National Security

In view of the current limitations of the assessment method, it needs to be further improved. The author believes that the construction of data exit security audit rules in China should be combined with Chinese specific national conditions. At the same time, we can refer to the experience of EU and the United States, further enrich the data exit audit mode in addition to the exit audit strategy of "one case, one discussion", and constantly improve and refine the standards and procedural requirements of China's exit audit, so as to protect national security more effectively. Specific ideas can be improved as follows:

First, formulate the rules of data flow regulation based on the current situation and needs of the development of China's digital economy. A country's position on the cross-border flow of data is closely related to the development of its digital trade. Generally speaking, in order to further facilitate the world

expansion of domestic enterprises, the advanced developing countries of digital economy industry tend to advocate the cross-border free flow of data. However, countries with weak development have no strong practical need for cross-border free flow of data. In China, the development of digital economy does not match the scale of cross-border data flow. From the perspective of domestic industrial development, technology companies such as Alibaba, Tencent and Huawei have formed leading advantages in the field of digital trade. However, according to McKinsey's calculation, when China's digital economy scale ranks the second-largest market in the global digital economy, the data flow in the network only ranks the eighth in the world, only 20% of that in the United States [19]. Compared with the huge volume of data economy, the scale of data flow in China is too small. Therefore, when constructing and improving the legal rules of cross-border data flow, China should appropriately relax the restrictions, standards and requirements on cross-border data flow on the basis of careful risk control.

Second, implement the national security risk control responsibilities of relevant subjects in the process of data exit, and make up for the ambiguity of the rules. Data exit security review should not only impose the review responsibility on the administrative department, but should establish a "trinity" review organization system of government departments, industry self-discipline organizations and data exit implementation subjects. The reason is that the data exit is closely connected with the scene of economic activities, the data has the characteristics of virtual, and the ways of exit are also rich and diverse. It is difficult to timely respond to the emerging data exit scenarios only relying on the industry regulatory authorities. Even at the rule level of data exit security review, due to the abstraction and limitations of the rules themselves, it is inevitable to have omissions or fail to guide the behavior of data exit implementation subjects from the practical level, resulting in the loss of operability. In view of the fact that the industry self-regulatory organizations are familiar with the scenarios and methods of data exit in the industry, and in practice, in other regulatory fields, especially the professional industry associations such as securities industry association and fund industry association, the industry self-regulatory organizations have played a good role in self-regulation by issuing self-discipline rules and operational norms. Therefore, we can consider giving the self-regulatory review function to the industry self-regulatory organization in the data exit safety review, including the self-regulatory organization further refining the data exit review rules established in relevant laws and regulations by formulating the exit review operation guide according to the specific characteristics of the industry data, so as to provide detailed and operable compliance guidance for the data exit implementation enterprises.

Third, soften the "one case, one discussion" mechanism in data exit security review, promote data flow, and give data subjects more predictability and reduce the burden of compliance. In order to meet the data exit demand and reduce the burden of data exit security review, it can be considered to provide additional flexible review strategies for some data exit reviews that are not closely related to national security in addition to the prior review mode. In the setting of an alternative review strategy, we can consider learning from the white list system and sufficient safeguard measures of GDPR as a supplementary review mechanism for data exit. On the one hand, some regions are included in countries and regions that can move freely through the "white list system". However, it should be noted that the white list itself should be flexible, and systems such as regular evaluation and temporary evaluation should be established to ensure that data inflow countries always maintain high standards of data protection. If data is transmitted to countries outside the white list, data can flow across borders as long as data controllers and data processors promise to provide adequate data protection measures [20].

5. Conclusion

In the process of constructing data exit security review rules, China should deal with the balance between national security maintenance and the international development of the digital economy. On the one hand, data security is closely related to national security. In the scenario of data exit, only by constructing relatively complete security audit rules can we provide a solid institutional foundation for the effective maintenance of national security. On the other hand, data exit is an important part of the international development of digital economy. When constructing data exit security review rules, we must consider the convenience of data exit. Although China tries to make a breakthrough in legislation by formulating norms such as the Measures, there are still some provisions that need to be improved and explained. In view of the limitations of China's data exit security review, such as the review mode being too single and the review rules have not being fully established, there is an urgent need for targeted improvement in China. We can learn from the relevant legislative practice of EU and American to establish the white list system and other normative measures in combination with China's specific national conditions, so as to meet the needs of China's digital economy development to the greatest extent on the basis of ensuring China's national security.

References

[1] World Economic Forum, Cross-Border Data Flows, Digital Innovation, and Economic Growth. http://reports.weforum.org/global-information-technology-report-2016/1-2-cross-border-data-flows-digital-innovat ion-and-economic-growth/, 2016 (accessed 1 December 2021）.

[2] Frost & Sullivan, Mega Trends in LATAM, Forecast to 2025. https://store.frost.com/mega-trends-in-latam-forecast-to-2025.html, 2017 （accessed 1 December 2021）.

[3] World Economic Forum, Global Information Technology Report 2016. https://www.weforum.org/agenda/2016/07/free-flow-of-data-between-countries/, 2016 (accessed 1 December 2021）.

[4] Robert Pepper, etc., Cross-Border Data Flows, Digital Innovation, and Economic Growth, in The Global Information Technology Report 2016. http://www3.weforum.org/docs/GITR2016/WEF_GITR_Chapter1.2_2016.pdf, 2016 (accessed 30 November 2021）.

[5] Cisco, Global Cloud Index: Forecast and Methodology, 2016–2021 White Paper. https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-7380 85.html, 2018 (accessed 30 November 2021）.

[6] Ouyang, Qiumei, WU Chao, Comparison and Application Prospect of Big Data and Traditional Security Statistics, China Safety Science Journal. 3 (2016) 1-7.

[7] L Xiaonan, Song Yang, Research on Data Exit Review Rules from the Perspective of National Security, Journal of Intelligence. 10 (2021) 74-82.

[8] L. Xiaonan, Trusted AI Justice: Significance, Challenge and Governance Responses, Legal Forum. 35 (2020) 116-126.

[9] Farrell, Henry, Negotiating Privacy Across Arenas: The EU-U.S. "Safe Harbor" Discussions, in: Adrienne Hdritier (Eds.), Common Goods: Reinventing European and International Governance, Rowman & Littlefield, Maryland, 2002, pp. 105-126.

[10] EAR, 15 C.F.R. § 730.5(c).

[11] Bureau of Industry and Security, Commerce, Review of Controls for Certain Emerging Technologies. https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies, 2018 (accessed 29 November 2021).

[12] National Archives, Controlled Unclassified Information. https://www.archives.gov/cui (accessed 29 November 2021).

[13] The United States Department of Justice, CLOUD Act. https://www.justice.gov/dag/cloudact (accessed 28 November 2021).

[14] Tambiama Madiega, Digital sovereignty for Europe. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf, 2020 (accessed 28 November 2021).

[15] Regulation (EU) 2018/1807 of the European Parliament and of The Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, L 303/59.
[16] Shi Jingxia, Zhang Duo, National security issues of cross-border data flow regulation, Social Sciences in Guangxi, 8 (2018) 128-133.
[17] European Commission, Binding Corporate Rules. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en (accessed 28 November 2021).
[18] Article 2, National Security Law of the People's Republic of China.
[19] McKinsey Global Institute, China and the world: understanding changing economic ties. https://www.mckinsey.com/~/media/mckinsey/featured%20insights/china/china%20and%20the%20world%20inside%20the%20dynamics%20of%20a%20changing%20relationship/mgi-china-and-the-world-full-report-feb-2020-en.pdf, 2019 (accessed 28 November 2021).
[20] Ma Qijia, Li Xiaonan, Research on Regulatory Rules of Cross Border Data Flow in the Context of International Digital Trade, International Trade, 3 (2021) 74-81.