J. East Asia & Int'l L. Vol. 17/No.1 (2024); 109-128
Publication type : Research Article
Section : Articles
DOI : http://dx.doi.org/10.14330/jeail.2024.17.1.06

China's Law and Policy on Cross-border Data Flow: A Review of Digital Silk Road

Ye Liu*

With the increasing value of data and the growing power in the field of digital economy, China has taken the governance of cross-border data flow(CBDF) as an important national strategy. At the domestic policy level, China has piloted Beijing, Shanghai, Hainan and Xiongan New Area to create international data centers with the intention to control inbound and outbound data resources. At the domestic legislative level, China insists that the outbound data transfers be conducted in a secure environment. At the international cooperation level, on the basis of the Global Data Security Initiative, China builds the consensus of countries and promotes cooperation among countries along the Belt and Road routes on CBDF through the Digital Silk Road. Simultaneously, China will engage proactively in the newly international economic and trade agreements, with RCEP standing as a prime example. China's discourse and model on CBDF governance have been continuously enhanced.

Keywords
China's Approach to CBDF, International Data Center, Security Assessment, Digital Silk Road, China-ASEAN Information Harbor

* Ph.D. candidate in law at the Xiamen University. LL.B.(ZNUEL), LL.M. (Xiamen U.). ORCID: http://orcid.org/0009-0007-2786-2160. The author may be contacted at: lyinsight@163.com /Address: No. 422, Siminnan road, Simin District, Xiamen, Fujian Province, 361005, P. R. China.
All the websites cited in this article were last visited on April 4, 2024.

I. Introduction

China's digital economy, which account as for 41.5% of China's GDP now,[1] has seen a significant speedup in the past decade. According to the 2023 Research Report on the Development of China's Digital Economy released by the China Academy of Information and Communications Technology (CAICT), the scale of China's digital economy increased rapidly from CNY 27.2 trillion in 2017 to CNY 50.2 trillion in 2022, nearly doubled in five years.[2] Benefited by the friendly domestic policies and large volume of digital internal market, many Internet technology companies has developed within a short period, such as Alibaba, Tencent, Baidu, ByteDance, Huawei, etc. These high-tech companies have not only dominated the internal market, but also ranked the second in the competition for the global digital market, only following the American companies.[3]

Meanwhile, the advantageous market condition with 1.4 billion proficient Internet users, has been attracting numerous foreign tech enterprises to invest in China. As the international digital economic and trade activities are based on cross-border data flow (CBDF), tech companies must obey China's regulatory policies on CBDF if they pursue expanding overseas. These years, China has taken many measures with respect to CBDF: at the policy level, China strongly supports and promotes local governments to pilot the reform policies, for building a series of international data centers, such as international big data exchange centers, international digital trading ports, cross-border e-commerce comprehensive pilot zones and other global data collecting and circulating hub centers; at the legislation level, China has constructed the legal framework of CBDF during these years, which put the "security assessment" as the core of the regulatory framework.[4]

At the international cooperation level, meanwhile, based on the Global Initiative on Data Security and the Digital Silk Road, China has continuously strengthened its international cooperation and consensus with Arabian countries, Association of Southeast Asian Nations (ASEAN) and Central Asian countries in the field of data governance. It has also been actively participating in the new generation of

1 China Academy of Information and Communications Technology, Research Report on the Development of China's Digital Economy (2023) [中国数字经济发展研究报告(2023年)], at 10, http://www.caict.ac.cn/kxyj/qwfb/bps/202304/P020230427572038320317.pdf.

2 *Id.*

3 Jeff Desjardins, *Visualizing the World's 20 Largest Tech Giants*, Visual Capitalist (July 6, 2018), http://www.visualcapitalist.com/visualizing-worlds-20-largest-tech-giants.

4 Jinhe Liu, *China's Data Localization*, 13(1) Chinese J. Commc'n 87-8 (2020).

digital economic and trade agreements, such as Regional Comprehensive Economic Partnership (RCEP) and Digital Economy Partnership Agreement (DEPA). China's influence in the formulation of digital rules is steadily growing, who has become one of the critical players in the international community in terms of the CBDF governance.

This research will mainly discuss China's CBDF from three levels respectively such as policy practice, legal framework and international cooperation. This paper is composed of five parts including Introduction and Conclusion. Part two will examine policy practices on CBDF in China. Part three will analyze the Legal Framework of Outbound Data Transfers. Part four will deal with China's International Cooperation on CBDF

II. Policy Practices on CBDF in China

China is placing growing emphasis on the fundamental role of data in the digital economy's innovative development, considering data as an essential productive factor including land, labor, technology, and capital. Hence, the Chinese government is actively taking measures to promote data utilization. In August 2020, the PRC Ministry of Commerce issued the Overall Pilot Plan for Comprehensively Deepening the Innovative Development of Trade in Services, in which four pilots of Beijing, Shanghai, Hainan and Xiongan New Area have been selected to explore the security management models of CBDF under the oversight of the Office of the Central Cyberspace Affairs Commission.[5]

A. The Beijing Pilot

As a benchmark city in the global digital economy, Beijing is leading other cities while establishing the data factor market. In 2021, the Beijing International Big Data Exchange was established. The Beijing Municipal Committee and the Beijing Municipal Government jointly issued the Implementation Opinions on Better Playing the Role of Data Factor and Further Accelerating the Development of the Digital Economy in June 2023, the Section 13 of which underlined the need to take the lead

5 PRC Ministry of Commerce, Notice on Printing and Distributing the Overall Pilot Plan for Comprehensively Deepening the Innovative Development of Trade in Services [关于印发全面深化服务贸易创新发展试点总体方案的通知] (Aug. 12, 2020), http://www.gov.cn/zhengce/zhengceku/2020-08/14/content_5534759.htm.

in exploring CBDF approaches.[6] Beijing focuses on constructing digital infrastructure for the sake of facilitating data accumulation.

Multinational enterprises are encouraged to construct data operation platforms by utilizing the existing cloud computing infrastructure. Haidian District is designed as the Beijing digital trading port and is going to construct the safe and convenient "dedicated channels" of the Internet. Chaoyang District is supported to build a data circulation service center for multinational enterprises in Beijing Central Business District, while Airport Economic Zone of Beijing Daxing International Airport is mapped out as the digital trade pilot zone.[7] Beijing is bending over backwards to strengthen international cooperation on the governance of CBDF; establish the mutual trust mechanism of data; and strive to build the digital trade port as one of the international leading "digital special zone."[8]

B. The Shanghai Pilot

As the first node for foreign data entering the domestic market, as well as an international well-known metropolis, Shanghai has unique advantages in CBDF governance. In August 2019, the Overall Plan for the Lingang New Area of the China (Shanghai) Pilot Free Trade Zone was issued by the State Council,[9] which stressed the necessity of ensuring the safe and orderly CBDF in the global Internet. The Plan mainly focuses on the construction of digital infrastructure.

In March 2021, Administrative Committee of the Lingang New Area officially planned to support the enterprises in the specific industries, such as the intelligent connected vehicle, industrial Internet and financial trade, to explore and proceed CBDF in Lingang. Furthermore, the construction of an integrated data service platform planned by this Committee includes the data center, Internet exchange center and dedicated channels of data flow.[10] Subsequently, the Committee proposed to build

6 Beijing Municipal Committee of the Communist Party of China and Beijing Municipal People's Government, The Implementation Opinions on Better Playing the Role of Data elements and Further Accelerating the Development of Digital Economy [关于更好发挥数据要素作用进一步加快发展数字经济的实施意见] (June 20, 2023), http://www.beijing.gov.cn/zhengce/zhengcefagui/202307/t20230719_3165748.html.

7 *Id.*

8 Haidian District People's Government of Beijing Municipality, Haidian Actively Explores the Construction of the Digital Trade Port [海淀积极探索数字贸易港建设] (Jan. 26, 2021), http://zyk.bjhd.gov.cn/ywdt/bmdt/202101/t20210126_4449817.shtml.

9 PRC State Council, The Overall Plan for Lingang New Area of China (Shanghai) Pilot Free Trade Zone [中国(上海)自由贸易试验区临港新片区总体方案] (Aug. 6, 2019), http://www.gov.cn/zhengce/content/2019-08/06/content_5419154.htm.

10 Administrative Committee of the Lingang New Area, 14th Five-Year Plan for the Digital Development of Lingang New Area of China (Shanghai) Pilot Free Trade Zone [中国(上海)自由贸易试验区临港新片区数字化发展 "十四五" 规划] (Mar. 30, 2021), at 13, http://www.lingang.gov.cn/upload/1/dm/1657698593163.pdf.

Lingang as an "International Data Port" with six functions including the outbound and inbound data transfer.[11]

In terms of inbound data transfer, Lingang tries to break through the CBDF barriers by either achieving mutual recognition of data protection with those developed countries, or attracting multinationals to set up headquarters in China. The Shanghai Municipal Government further emphasized the construction of the "International Data Port" with convenient cross-border interaction of industrial aggregation, display and transaction.[12] The construction of International Data Port was officially written into the Lingang New Area Regulation of China (Shanghai) Pilot Free Trade Zone in 2022.[13] Based on the Lingang pilot, the Regulation will promote the construction of the International Data Port; build the new digital infrastructure; and strive to build a global data collection and circulation hub platform.[14] At the same time, it also explores a low-risk list of CBDF in the Lingang New Area.[15]

C. The Hainan Pilot

The Hainan Free Trade Port is a pioneer in implementing the policies of comprehensively deepening the economic reform and testing the highest level of opening-up. In June 2020, the Central Committee and the State Council issued the Overall Plan for the Construction of Hainan Free Trade Port.[16] The institutional framework of this Overall Plan consists of "six freedoms," among which special focus is put on the freedom of trade, investment and data. The safe and orderly data flow is an important factor to evaluate the high opening-up of Hainan Free Trade Port. On the premise of ensuring the safe and orderly data flow, it is proposed to expand the opening field of data; innovate the security system design; realize the full convergence

11 Management Committee of Lingang New Zone, "14th Five-Year" Special Plan for Digital Economy Industry Innovation and Development in Lingang New Area of China (Shanghai) Pilot Free Trade Zone [中国(上海)自由贸易试验区临港新片区数字经济产业创新发展 "十四五" 专项规划] (May 12, 2021), http://www.lingang.gov.cn/html/website/lg/index/government/juecegongkai/paln/index.html.

12 Shanghai Municipal Government, The 14th Five-Year Plan for the Development of Lingang New Area of China (Shanghai) Pilot Free Trade Zone [中国(上海)自由贸易试验区临港新片区发展 "十四五" 规划] (July 21, 2021), http://www.shanghai.gov.cn/nw12344/20210812/bd6b7c5e895d42ac8885362bd0ae6e0c.html.

13 Standing Committee of Shanghai Municipal People's Congress, Lingang New Area Regulation of China (Shanghai) Pilot Free Trade Zone [中国(上海)自由贸易试验区临港新片区条例] (Feb. 18, 2022), http://www.spcsc.sh.cn/n8347/n8467/u1ai242732.html.

14 Lingang New Area Regulation of China (Shanghai) Pilot Free Trade Zone, art. 32.

15 *Id*. art. 33.

16 The CPC Central Committee and the State Council, The Overall Plan for the Construction of Hainan Free Trade Port [海南自由贸易港建设总体方案] (June 1, 2020), http://www.gov.cn/zhengce/2020-06/01/content_5516608.htm.

of data and cultivate the digital economy.[17]

D. The Xiongan New Area Pilot

As an representative of the new generation of modern city carrying on Beijing's non-capital functions, Xiongan New Area in Hebei province is positioned as the digital intelligent city, the world-class innovation city, and the green and low-carbon city.[18] In the field of CBDF, Xiongan mainly focuses on the cross-border e-commerce, for the purpose of realizing the free CBDF on the whole industrial chains of cross-border e-commerce. In July 2020, the Hebei Provincial Government issued the Implementation Plan for the Construction of China (Xiongan New Area) Cross-border E-commerce Comprehensive Experimental Zone, underlining the establishment of an international information sharing system.[19] Relying on the construction of the intelligent city, Xiongan establishes a record-filing information sharing system for cross-border e-commerce enterprises and unifies the standards and norms of information, so that the record-filing information of enterprises can be checked by each other in every chain of e-commerce.[20]

Furthermore, Xiongan is exploring an information traceability system for import and export commodities. This system will aim to collect data from all stages and oversee the entire e-commerce chains. Actually, the CBDF regulatory policy of China focuses on "security goals," while each pilot can only promote the free CBDF under the premise of ensuring data security. Since the regulatory authority to outbound data transfers belongs to the competent central government, these pilots are subject to the regulatory restrictions already set by the central government, which have only the limited discretion to make it easier to transfer data overseas.[21]

As a consequence, these pilots would like to focus on inbound data transfers, and create complete digital infrastructures and excellent business environment to attract tech enterprises overseas to settle in China. In this way, overseas data may

17 *Id.* at ¶ 18.

18 Chinese State Council, On the Approval of the Overall Plan of Xiongan New Area in Hebei Province (2018-2035) [关于河北雄安新区总体规划(2018-2035年)的批复] (Dec. 25, 2018), http://www.gov.cn/zhengce/content/2019-01/02/content_5354222.htm.

19 Hebei Provincial Government, Implementation Plan for the Construction of China (Xiongan New Area) Cross-border E-commerce Comprehensive Experimental Zone [中国(雄安新区)跨境电子商务综合实验区建设实施方案] (July 7, 2020), http://www.xiongan.gov.cn/2020-09/01/c_1210780669.htm.

20 *Id.*

21 Nianli Zhou, Meiyue Yu & Chunmiao Liu, *Research on the System Innovation of the Pilot Construction of Cross-border Data Flow in China's Free Trade Zone* [我国自贸区(港)数据跨境流动试点制度创新研究], 44(4) Int'l Bus. Res. 90-1 (2023).

gradually flow into China. The legal framework of outbound data transfers is mainly formulated by the Cyberspace Administration of China (CAC).

III. The Legal Framework of Outbound Data Transfers

A. An Overview

Along with the increasing attention of Chinese governments on CBDF, relevant legislations have been enacted promptly these years in China. China has formed a multi-level and systematic legal framework for CBDF, including laws, administrative regulations, national standards and guidelines. The laws include the Cyber Security Law,[22] the Data Security Law,[23] and the Personal Information Protection Law.[24] These three laws construct the top-level design of CBDF in China. Administrative regulations are as follows: the Security Protection Regulations for Critical Information Infrastructure,[25] the Cybersecurity Review Measures,[26] the Security Assessment Measures for Outbound Data Transfers,[27] the Implementation Rules for Personal Information Protection Certification,[28] and the Measures on the Standard Contract for Outbound Transfer of Personal Information,[29] are the detailed implementation rules for the top-level design. The Information Security Technology-Personal Information Security Specification,[30] the Information Security Technology - a draft Guideline for

22 The NPC Standing Committee, Cybersecurity Law of the People's Republic of China [中华人民共和国网络安全法] (Nov. 7, 2016), http://www.npc.gov.cn/c2/c30834/201905/t20190521_274248.html.

23 The NPC Standing Committee, Data Security Law of the People's Republic of China [中华人民共和国数据安全法] (June 10, 2021), http://www.npc.gov.cn/npc/c2/c30834/202106/t20210610_311888.html.

24 The NPC Standing Committee, Personal Information Protection Law of the People's Republic of China [中华人民共和国个人信息保护法] (Aug. 20, 2021), http://www.npc.gov.cn/c2/c30834/202108/t20210820_313088.html.

25 PRC State Council, Security Protection Regulations for Critical Information Infrastructure [关键信息基础设施安全保护条例] (July 30, 2021), http://www.gov.cn/gongbao/content/2021/content_5636138.htm.

26 Cyberspace Administration of China, Cybersecurity Review Measures [网络安全审查办法] (Dec. 28, 2021), http://www.cac.gov.cn/2022-01/04/c_1642894602182845.htm.

27 Cyberspace Administration of China, Security Assessment Measures for Outbound Data Transfers [数据出境安全评估办法] (July 7, 2022), http://www.cac.gov.cn/2022-07/07/c_1658811536396503.htm.

28 Cyberspace Administration of China, Implementation Rules for Personal Information Protection Certification [个人信息保护认证实施规则] (Nov. 18, 2022), http://www.cac.gov.cn/2022-11/18/c_1670399936983876.htm.

29 Cyberspace Administration of China, Measures on the Standard Contract for Outbound Transfer of Personal Information [个人信息出境标准合同办法] (Feb. 22, 2023), http://www.cac.gov.cn/2023-02/24/c_1678884830036813.htm.

30 Standardization Administration, Information Security Technology-Personal Information Security Specification [信息安全技术 个人信息安全规范] (Mar. 6, 2020), http://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=4568F276E0F8346EB0FBA097AA0CE05E.

Identification of Critical Data,[31] the Guideline of Security Assessment Declaration for Outbound Data Transfers (first edition),[32] and the Security Certification Specification of Personal Information Cross-border Processing Activities v2.0.[33] They are national standards or guidelines that provide more detailed practical guidance for governments and enterprises.

In general, the legal framework of outbound data transfers might be applied from four steps. Firstly, identify whether the data exporter is a critical information infrastructure(CII) provider. If yes, as long as there are any data to export, the security assessment of outbound data transfers is required.[34] Secondly, if the data exporter is not a CII provider, the question is to identify whether the data is the key data. If yes, regardless of the amount of data to be transferred, there is a necessity for security assessment.[35] Thirdly, if the data exporter is not a CII provider and the data exported are not key data, it should be then identified whether the data exporter is the personal information processor with a specific amount of personal information.[36] If the amount of personal information does meet the requirement, the data exporter should carry out the security assessment. At the end of the fourth step, if none of the above is possible, the exporter of personal information should choose their compliance methods according to the specific business scenarios.[37]

In summary, from the first step to the third step, the data exporter should apply security assessment of outbound data transfers, while in the last step, the data exporter may choose standard contract or personal information protection certification. In the practical scenarios of CBDF, the data exporter could adopt appropriate legal approaches according to the specific scenario through the above "four-step" analysis. There are three legal tool for data export including security assessment, standard contract and personal information protection certification.[38]

31 National Information Security Standardization Technical Committee, Information Security Technology-a draft Guideline for Identification of Critical Data [信息安全技术 重要数据识别指南（征求意见稿）] (Jan. 13, 2022), http://www.tc260.org.cn/front/bzzqyjDetail.html?id=20220113195354&norm_id=20201104200036&recode_id=45625.

32 Cyberspace Administration of China, Guideline of Security Assessment Declaration for Outbound Data Transfers (first edition)[数据出境安全评估申报指南(第一版)](Aug. 31, 2022), http://www.cac.gov.cn/2022-08/31/c_1663568169996202.htm.

33 National Information Security Standardization Technical Committee, Security Certification Specification of Personal Information Cross-border Processing Activities v2.0 [个人信息跨境处理活动安全认证规范V2.0] (Dec. 16, 2022), http://www.tc260.org.cn/front/postDetail.html?id=20221216161852.

34 Security Assessment Measures for Outbound Data Transfers, art. 4(2).

35 *Id*. art. 4(1).

36 *Id*. art. 4(2)&(3).

37 Personal Information Protection Law art. 38 (2)&(3).

38 *Id*. art. 38.

B. Security Assessment

1. The Applicable Scenarios of the Security Assessment

According to Article 4 of the Security Assessment Measures for Outbound Data Transfers, and combined with the "four-step" analysis above, the security assessment is mainly concerned with the first three steps and surrounds the identification of three important concepts. The first is the identification of "CII providers." Critical information infrastructure refers to:

> [t]he important network facilities and information systems in important industries and fields such as public telecommunications, information services, energy, transportation, water conservancy, finance, public services, e-government and national defense science, technology and industry, as well as other important network facilities and information systems which, in case of destruction, loss of function or leak of data, may result in serious damage to national security, the national economy and the people's livelihood and public interests.[39]

As this definition of CII does not exclude private entities, even private providers have the possibility to be identified as CII providers as long as their network facilities or information systems may seriously endanger national security or public interest if attacked.

The second is the identification of "key data"(critical data). Key data refers to "the data that exists in an electronic way, may endanger national security and public interest once tampered with, damaged, leaked, illegally obtained or used.[40] The Guideline defines "key data" simply as the "national security" and "public interest." It will lead to the concept of "key data" too abstract and ambiguous to identify in practice.[41] Moreover, although the Guideline explicitly emphasize that "key data" does not include "state secrets" and "personal information," these concepts may overlap with each other given their definition criteria are not consistent with each other.

The third is the identification of "personal information processors which process a specific amount of personal information." "Personal information refers to all kinds of information related to identified or identifiable natural persons recorded by electronic or other means,"[42] while identifying "a data processor processing the personal

39 Security Protection Regulations for Critical Information Infrastructure, art. 2.

40 Information Security Technology- Draft Guideline for Identification of Critical Data, art. 3.

41 Gaofeng Zhu, *Understanding and Identification: Defining key Data and Selecting its Regulatory Approach* [认识与识别：重要数据的界定及其规制路径选择], 38(6) Soc. Sci. [社会科学家] 106 (2023).

42 Personal Information Protection Law, art. 4.

information of more than one million people" does not mean that the date processor needs to have more than one million users.[43] As long as the processing of personal information involves one million people, the security assessment shall be required. It is not difficult for some Internet tech companies to reach this threshold, especially for those who provide digital services for consumers. The threshold for identifying a data processor who "has provided personal information of 100,000 people or sensitive personal information of 10,000 people in total abroad since January 1 of the previous year" is even lower.[44]

Personal sensitive information includes personal property information, personal health physiological information, personal biometric information, personal identity information, sexual orientation, friends list, whereabouts, web browsing records and other personal information that may endanger personal and property safety, or easily cause damage or discriminatory treatment to personal reputation, physical and mental health once leaked, illegally provided or abused.[45] The list of personal sensitive information encompasses a vast majority of personal data that a data subject has produced in cyberspace. As a result, most personal data can be categorized under this label, which essentially removes the distinction or threshold for 100,000 individuals. More than one year, security assessment only requires the total personal information of more than 10,000 people. This may lead to the logical consequence that almost all the scenarios of the personal information export will be under the control of security assessment.

2. Implementation of Security Assessment

First, the applicant's pre-existing risk self-assessment should be conducted. Before applying for the security assessment, the applicant needs to assess its risk of outbound data transfers and submit a written report of risk self-assessment.[46] The self-assessment generally includes the following aspects: first, the legality, legitimacy and necessity of the outbound data transfer and data processing in question; second, the risk assessment of the outbound data transfer related to national security, public interests or the legitimate rights and interests of individuals or organizations; third, the assessment of the data security capability of the overseas recipient; fourth, the channels for the maintenance of personal information rights and interests; fifth, the assessment to the data security obligations of the relevant contracts concluded with

43 Security Assessment Measures for Outbound Data Transfers, art. 4(2)&(3).

44 *Id*. art. 4.

45 Information Security Technology-Personal Information Security Specification, art. 3.2.

46 Security Assessment Measures for Outbound Data Transfers, art.5.

the overseas recipient.[47] The risk self-assessment report is one of the necessary written materials for the application of security assessment.

The formal and substantial security assessment comes next. The formal security assessment is conducted by the provincial cyberspace departments, which mainly examines the completeness of the application materials submitted by the applicant, including the application form, the risk self-assessment report and the legal documents concluded with the overseas recipient.[48] After passing the formal security assessment, the CAC will be responsible for the substantive security assessment.[49] Compared with the applicant's risk self-assessment, the substantial security assessment also assesses the data security protection policies, regulations and network security environment of the country where the recipient locates in.

Additionally, it is a crucial factor for the substantial security assessment to consider whether the recipient can provide the protection standards that are on par with China's data protection legal system.[50] Overseas recipient is required to provide the same data protection standard. Besides, the substantial security assessment also examines the law-abiding records of the applicant in China. The applicant with illegal records will confront more challenges to pass the security assessment.[51] The power of substantial security assessment is under the control of CAC, while the local cyberspace departments are only responsible for the formal review. This reflects the fact of consolidating and strengthening the central authority for outbound data transfers. The assessment mechanism seriously hinders the approval efficiency of security assessment. From September 2022 to June 2023, only 13 enterprises were approved by the CAC, including 3 enterprises in Beijing, 2 in Shanghai, 3 in Zhejiang, 3 in Guangdong, and 1 each in Shandong and Jiangsu. The enterprises involved are mainly in the fields of e-commerce, retail, automotive and electronic technology as well.[52]

Finally, the re-assessment could be divided into expired re-assessment and dynamic re-assessment. The former means that the applicant should be re-assessed after the expiration of the two-year's validity period, while the latter means the re-assessment should be done when the assessment factors change within the validity period. The trigger conditions of dynamic re-assessment might be divided into the

47 *Id.*

48 *Id.* arts. 6 & 7.

49 *Id.* art. 10.

50 *Id.* art. 8(2).

51 *Id.* art. 8(6).

52 Liao Quan, Up to Now, more than 10 Enterprises have Passed the Data Exit Safety Assessment [截至目前已超过10家企业通过数据出境安全评估] (June 30, 2023), http://mp.weixin.qq.com/s/fexv032v1VCzpcLKB7KDEQ.

active self-investigation and the passive reporting supervision. In terms of self-investigation, when the security assessment factors have changed substantially within the validity period, it is necessary for the recipient to apply for re-assessment on its own initiative.[53] With regard to the passive reporting supervision, any organization or individual who perceives the applicant's violation of law may report to the cyberspace department concerned.[54] If the applicant is investigated that it fails to meet the requirements of security assessment, the cyberspace department has the authority to terminate the data exporting activities of the data exporter until it has rectified as required.[55]

C. Personal Information Protection Certification

The certification system is a third-party assessment system that aims to respond to the information asymmetry in the market economy and reduce the credit cost in transactions. According to the transparent and authoritative technical standards and norms, the third-party organization with professional competence shall make an assessment for the qualifications, products or services of the data exporter, so as to facilitate the smooth development of market activities.[56] Article 38 of the Personal Information Protection Law stipulates that the personal information processor could choose the personal information protection certification as a legal tool for outbound personal information transfers when the processor does not meet requirements of the security assessment.

In November 2022, the State Administration for Market Regulation and the CAC jointly issued the Announcement on the Implementation of Personal Information Protection Certification. The technical standard documents used for certification are the Information Security Technology-Personal Information Security Specification and the Personal Information Security Certification Specification of Cross-border Processing Activities.[57] The main processes of personal information protection certification are the technical verification, on-site audit and post-certification supervision.[58]

During the validity period of 3 years of certification, the certified personal information processor is continuously supervised to ensure that it continues to

53 Security Assessment Measures for Outbound Data Transfers, art. 14.

54 *Id*. art. 16.

55 *Id*. art. 17.

56 National Research Council et al., Certifiably Sustainable?: The Role of Third-party Certification Systems: Report of a Workshop (2010), at 3-5, https://nap.nationalacademies.org/catalog/12805/certifiably-sustainable-the-role-of-third-party-certification-systems-report.

57 Implementation Rules for Personal Information Protection Certification, art. 2.

58 *Id*. art. 3.

meet the certification requirements. For the certification of cross-border processing activities, though it only targets the domestic personal information processor, the overseas recipient is also required to meet the certification requirements at the substantial level. For example, the Personal Information Security Certification Specification of Cross-border Processing Activities (2nd edition) requires the personal information processor and the overseas recipient to sign legally binding and enforceable documents; designate a representative in charge of personal information protection; set up personal information protection agencies; and abide by consistent rules for cross-border processing of personal information.[59] In addition, the personal information processor should conduct the impact assessment of personal information protection as well.[60]

Since the personal information protection certification is valid for three years after obtaining the certificate, the applicable CBDF scenarios for certification mainly feature low-risk, frequent cross-border flow and basic information processing activities. Due to the minimum quantity limitation of personal information to initiate a security assessment, companies with the personal information protection certification typically do not engage in businesses directly related to data subjects, or they have to keep their businesses at a limited scale. It is more suitable for the personal information protection certification to be used in the data flow between companies belonging to the same multinational group, and data flow with respect to the cooperation of companies in the specific ecosystems.[61]

D. Standard Contract

In the scenario of low-risk cross-border personal information flow, the data exporter can choose the standard contract in addition to the personal information protection certification.[62] The personal information protection certification is different from the standard contract which is generally applicable to occasional CBDF scenarios. In addition, the personal information protection certification is required for signing contracts or other legal documents between the data exporter and the overseas recipient. Most substantial protection of outbound data will eventually lead to civil liability relief when a contract with an overseas recipient is breached. The standard

59 Personal Information Security Certification Specification of Cross-border Processing Activities (2d ed.), art. 5.1- 5.3.

60 *Id*. art. 5.4.

61 Dengke Xie, *On the Corporate Compliance in Cross-border Supply of Personal Information* [个人信息跨境提供中的企业合规], 38(1) Legal F. [法学论坛] 93 (2023).

62 Personal Information Protection Law, art. 38.

contract is a basic and effective regulatory tool in the field of CBDF. This legal tool could not only realize the direct audit of important matters on CBDF, but also urge the overseas recipient to actively fulfill their obligations of data security protection based on the liability for breach of contract.[63]

In February 2023, the CAC issued the Measures on the Standard Contract for Outbound Transfer of Personal Information, along with the standard contract template. The Measures are similar to the security assessment procedures. Before signing the standard contract, the personal information processor is required to implement the impact assessment of personal information protection. The assessment factors are more comprehensive than the risk self-assessment of security assessment processes, but it is basically consistent with the factors of substantive security assessment conducted by the CAC.[64] Depending on the levels of risks of impact assessment, the data exporter can choose to either conduct a security assessment or continue using the standard contract.

After signing the standard contract, the data exporter shall submit the standard contract and the impact assessment report of personal information protection to the local cyberspace department, and perform the obligation of record-filing.[65] The record-filing system of standard contract is conducive to regulatory agencies to control the situations of outbound personal information in a timely and comprehensive manner, monitor the overseas risks, handle risk events and safeguard the security interests of the state, the public and individuals.[66]

IV. China's International Cooperation on CBDF

A. Geopolitical Phenomenon on CBDF

The differences in political and legal systems between western countries and China have imposed geographical restrictions on China in the field of CBDF, which increasingly evolved towards the direction of discrimination and exclusion to China.[67]

63 Jingwu Zhao, *The Construction Foundation and Regulatory Transformation of Standardized Contract in Cross-border Data Transmission* [数据跨境传输中标准化合同的构建基础与监管转型], 40(2) Legal Sci. (J. Nw. U. Pol. Sci & L. [法律科学(西北政法大学学报)] 149 (2022).

64 Measures on the Standard Contract for Outbound Transfer of Personal Information, art. 5.

65 *Id*. art. 7.

66 Jingwu Zhao, *On the Systematization of Data Cross-Border Assessment, Contracts and Authentication Rules* [论数据出境评估、合同与认证规则的体系化], 31(1) Admin. L. Rev. [行政法学研究] 81 (2023).

67 Yanqing Hong, *The Fragmentation of Rules for Cross-border Data Flows and China's Response* [数据跨境流动的规则碎

The current influential CBDF mechanisms of the international community are mainly represented by the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) and Asia-Pacific Economic Cooperation's (APEC) Cross-Border Privacy Rule system (CBPRs). The former was promoted under the EU's leadership, also based on the General Data Protection Regulation (GDPR).

In August 2023, the Convention 108 had been joined by 55 countries, comprising 46 Council of Europe members and 9 non-member states.[68] The latter, led by the US, has the common protection standard in CBDF under the APEC's Privacy Framework with a low level of protection. The CBPRs mainly involves Mexico, Canada, Japan, Singapore, South Korea, Australia, Chinese Taipei and other economies with close political links to the US.[69]

When it comes to Convention 108, the concept of human rights in Europe differs significantly from that in China and the differences between their protection mechanisms of personal data are more difficult to reconcile, such as restricting the access of the government to personal data. Additionally, the Convention 108 with distinct geopolitical tendency and the CBPRs is the product of the US's hegemony. The participating economies have to lower the legal protection standards for CBDF. Countries like Japan and Singapore have amended their domestic data protection laws to incorporate the lower protection standard of CBPRs into their legal systems equipped with higher protection standard.[70]

In Singapore, for example, Section 26(1) of its Personal Data Protection Act (PDPA) stipulates that any organization that transfers personal data abroad should ensure that it has provided a protection standard comparable to the PDPA, otherwise the data cannot be transferred abroad. Section 10(1) of the Personal Data Protection Regulation (PDPR) further explains that the data exporter must take appropriate measures to ensure that the overseas recipient is subject to legally enforceable obligations, which are at least comparable to the PDPA. When the overseas recipient becomes a member of CBPRs, the PDPR regards it as the one who have been subject to legally enforceable

片化及中国应对], 30(4) Admin. L. Rev. [行政法学研究] 69 (2022).

68 Non-Members of Council of Europe include Argentina, Cabo Verde, Mauritius, Mexico, Morocco, Russian Federation, Senegal, Tunisia and Uruguay. *See* Council of Europe, Chart of Signatures and Ratifications of Treaty 108, http://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108.

69 Cross-Border Privacy Rules, *Government*, http://cbprs.org/government.

70 Yanqing Hong, *China's Plan to Promote the Cross-border Data Flow along the "the Belt and Road": Based on the Paradigms of US and EU* [推进"一带一路"数据跨境流动的中国方案- 以美欧范式为背景的展开], 8(2) China L. Rev. [中国法律评论] 33 (2021).

obligations.[71]

B. China's Independent Path for International Cooperation on CBDF

At present, China mainly relies on the Digital Silk Road and the Global Data Security Initiative to build the international consensus on CBDF among countries along the Belt and Road routes; strengthen the regional cooperation on data governance and digital economy; and strive to build a free circle of CBDF under the Belt and Road Initiative.[72]

1. The Global Data Security Initiative and the Construction of China's Discourse

In 2020, China put forward the Global Data Security Initiative on the international society to resolve divergences on data security, privacy protection and economic development among countries. This Initiative is regarded as the blueprint of rules to build a framework of international digital and cyber rules accepted by all parties.[73] As a result, China and the League of Arab States (LAS) jointly issued the China-LAS Cooperation Initiative on Data Security in 2021.[74] In 2022, China and five Central Asian countries jointly issued the Data Security Cooperation Initiative of China+Central Asia.[75] These initiatives have created the opportunities for China, LAS and Central Asian countries to jointly promote global digital governance and international rule-making.

In February 2023, the PRC Ministry of Foreign Affairs further issued the Global Security Initiative Concept Paper and deepened the international cooperation in the field of information security. It jointly addresses various cyber threats, and "work(s) to establish a global governance system on cyberspace featuring openness and inclusion, justice and fairness, security and stability, vigor and vitality."[76] In addition, through

71 Personal Data Protection Regulation, § 12.

72 Longyue Zhao & Hongwei Gao, *China and Global Digital Trade Governance: Opportunities and Challenges Based on Joining DEPA* [中国与全球数字贸易治理：基于加入DEPA的机遇与挑战], 30(2) Pac. J. [太平洋学报] 23 (2022).

73 Chinese Ministry of Foreign Affairs, Global Data Security Initiative Inject New Impetus into Global Governance [《全球数据安全倡议》为全球治理注入新动力] (Nov. 24, 2020), http://world.people.com.cn/n1/2020/1124/c1002-31942744.html.

74 Chinese Ministry of Foreign Affairs, China-LAS Cooperation Initiative on Data Security [中阿数据安全合作倡议] (Mar. 29, 2021), http://bbs.fmprc.gov.cn/wjb_673085/zzjg_673183/jks_674633/fywj_674643/202103/t20210329_9176279.shtml.

75 PRC Ministry of Foreign Affairs, "China+Central Asia Countries" Data Security Cooperation Initiative ["中国＋中亚五国"数据安全合作倡议] (June 8, 2022), http://new.fmprc.gov.cn/web/wjbzhd/202206/t20220609_10700811.shtml.

76 PRC Ministry of Foreign Affairs, Global Security Initiative Concept Paper [全球安全倡议概念文件] (Feb. 21, 2023), http://www.mfa.gov.cn/wjbxw_new/202302/t20230221_11028322.shtml.

the 14th BRICS Summit's Beijing Declaration 2022, China is actively strengthening international cooperation with the BRICS countries in the field of cybersecurity governance.[77]

In November 2022, the PRC State Council issued an White Paper called Jointly Build a Community with a Shared Future in Cyberspace,[78] which comprehensively and emphatically explained the basic proposition and position of China on cyberspace governance and CBDF. China always "respects cyber sovereignty" and "advocates the principle of sovereign equality of the UN Charter applicable to cyberspace and establishes a fair and reasonable international order in cyberspace on the basis of national sovereignty."[79] In digital economy, China adheres to "creat(ing) an open, fair, just, non-discriminatory digital development environment. [...] jointly explor(ing) the formulation of international digital governance rules that reflect the wishes and interests of all parties."[80] In CBDF, "China supports data flow and data utilization, promotes the openness and sharing of data, provides the formulation of relevant international rules and standards under the bilateral and multilateral cooperation framework, continuously improves the interoperability between different prevailing data protection rules, and promotes the safe and free cross-borders data flow."[81]

2. Digital Silk Road and Regional Cross-border Data Flow

Under the design for the Digital Silk Road construction, which could provide important technical supports under the Belt and Road Initiative, China is actively building digital economy infrastructure and promoting the free flow of data in and among countries and regions along the Belt and Road. China has signed the MoU on Digital Silk Road cooperation with 16 countries; established bilateral cooperation mechanisms on Silk Road E-commerce with 22 countries; and launched or planned to launch relevant projects with 137 countries on Digital Silk Road so far.[82]

The construction of China-ASEAN Information Port is a typical case of the Digital Silk Road. The China-ASEAN Information Port is jointly built by China and

77 14th BRICS Summit Beijing Declaration [金砖国家领导人第十四次会晤北京宣言] (June 23, 2022), http://www.news.cn/world/2022-06/24/c_1128771000.htm.

78 PRC State Council, Jointly Build a Community with a Shared Future in Cyberspace [携手构建网络空间命运共同体] (Nov. 2022), http://www.gov.cn/xinwen/2022-11/07/content_5725117.htm.

79 *Id.*

80 *Id.*

81 *Id.*

82 Big Data Research Institute of Guangxi Zhuang Autonomous Region, *Analysis of Opportunities and Challenges and Countermeasures for the Construction of China-ASEAN Information Port* [中国—东盟信息港建设面临的机遇挑战分析和对策建议], 173(17) Res. Big Data & Decision Making [大数据与决策研究] 6 (2023), http://gxxxzx.gxzf.gov.cn/zybg/dsjjcyyj/2023n/P020230628311211787935.pdf.

the ASEAN countries. With the basic contents in deepening network connectivity, information exchange, cooperation and mutual benefit, China-ASEAN Information Port has been deemed as an information hub between China and ASEAN. In this regard, Guangxi province is an critical fulcrum of the Port. In 2021, the Guangxi Provincial Government issued the 2021-2025 Development Plan of "Digital Silk Road" towards ASEAN,[83] formally proposing to support the construction of Digital Silk Road with Guangxi as the fulcrum of the China-ASEAN Information Port. Then, Guangxi provincial government further required the Office of the Guangxi Cyberspace Affairs Commission and the Big Data Development Bureau to build an international data hub with ASEAN.[84] Some measures will be taken for exploring the mechanism of mutual recognition with the ASEAN countries in data security supervision; promoting the pilot construction on CBDF between China and ASEAN; and supporting the establishment of the whole-process security supervision mechanism on CBDF.[85]

In order to speed up the CBDF between China and other countries along the Belt and Road routes, China has begun to actively promote the data flow among different jurisdictions of Guangdong-Hong Kong-Macao Greater Bay Area (GBA), which is a meaningful attempt to accumulate useful experience for CBDF between China and other countries. In June 2023, the CAC and the Innovation, Technology and Industry Bureau (ITIB) of Hong Kong jointly signed the MoU on Facilitating Cross-boundary Data Flow within the Guangdong-Hong Kong-Macao Greater Bay Area.[86] Under the existing national security management framework to outbound data transfers, the MoU plans to establish the security system of CBDF in GBA.

This security system aims to promote the secure and orderly CBDF within the GBA. The legal systems of data protection in Hong Kong, Macao and Guangdong are different. The cross-border flow of personal information among these three different jurisdictions must be based on the compliance of outbound data transfers and the equal protection to personal information. Seeking solutions to these problems will undoubtedly offer valuable experience in aligning with other countries on data protection standards.

83 Guangxi Zhuang Autonomous Region Government, 2021-2025 Development Plan of "Digital Silk Road" towards ASEAN [广西面向东盟的"数字丝绸之路"发展规划(2021-2025年)] (Nov. 12, 2021), http://www.gxzf.gov.cn/zfwj/zxwj/t10807438.shtml.

84 Guangxi Zhuang Autonomous Region Government, Notice to 2022-2025 Implementation Plan of the Construction for China-ASEAN Information Port [中国-东盟信息港建设实施方案(2022-2025年)的通知] (Nov. 21, 2022), http://swt.gxzf.gov.cn/zfxxgk/fdzdgknr/zcyjd/gxzc/t14175577.shtml.

85 *Id.*

86 Xiang Ye, *Alibaba Cloud's Personal Information Cross-Border Compliance in GBA: A Perspective of Jurisdiction Concurrence* [阿里云在大湾区的个人信息跨境合规：管辖权竞合视角], 35(7) China Bus. & Mkt. [中国流通经济] 107 (2021).

3. China's Participation in RECP and Others

RCEP officially came into force in January 2022. Six ASEAN members and four non-ASEAN members including China, Japan, New Zealand and Australia have begun to implement it. RECP in operation marks the official establishment of the trade zone with the largest population and economic scale of the world. Just like the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and DEPA, RCEP adopts the basic position of free CBDF with the "free flow" as the principle[87] and the "restricted flow" as the exception.[88] At present, the legal regulation of China on CBDF put the priority on the national security and data security as the fundamental goal. The preference to the security causes the generalization of data security assessment; limits the outbound data transfer; and finally results in *de facto* data localization. It is inconsistent with the strategy for encouraging free CBDF in RCEP, CPTPP and DEPA.[89] In this regard, China needs to further clarify the scope of application of security assessment; define the core concepts such as CII, key data and personal sensitive information; avoid the generalization of security assessment; and truly realize the free CBDF in low-risk scenarios.

Furthermore, the clauses of "restricted flow" exception in RCEP attach more attention to the interests compared to those in CPTPP and DEPA, because RCEP parties will have more discretion to interpret and apply the exception clauses. On the one hand, RCEP introduces the "essential security interests" exception. According to RCEP, "[N]othing in this Article shall prevent a Party from adopting or maintaining" measures necessary to achieve "a legal public policy objective" and protect its "essential security interests."[90] Meanwhile, the parties have the discretion to judge the necessity of invoking the exception clauses and even counter any objections raised by other parties when invoking the exception of "essential security interests." Therefore, RCEP has little substantial impact on the domestic legislations of the countries who strictly restrict the outbound data transfers.[91]

However, with the further implementation of RCEP and the free value-oriented CPTPP and DEPA, China should adjust its domestic legal system in response to outbound data transfers, and align its laws with the relevant international rules. For instance, the special concepts and rules of international economic and trade

87 RCEP ch. 12, art.15, ¶ 2.

88 CPTPP art. 14.11; DEPA, module 4, § 4.3.

89 Xiaojun Zhang & Xiaomeng Qu, *The Exception Clauses of Cross-border Data Transfer in RCEP and China's Response* [RCEP数据跨境流动例外条款与中国因应], 38(3) Zheng Fa Lun Cong [政法论丛] 117(2022).

90 RCEP ch. 12, art. 15, ¶ 3.

91 Chengyu Zhang, *RCEP Basic Security Exceptions for Cross-Border Data Flows and China's Response*, 14 J. Educ. Human. & Soc. Sci. 39 (2023).

agreements, such as "essential security interests," should be incorporated into the domestic legislation to keep in line with international regulations.[92]

V. Conclusion

In the era of digital economy, data is the critical strategic resource for states. As a result, the strategic gaming in data resources between developed countries is becoming increasingly fierce. This phenomenon is mainly reflected in the field of CBDF. In the face of the geostrategic siege from the US and the EU, China is actively exploring the governance model of the community with a shared future. Based on the Digital Silk Road, China is developing cooperation practices with countries on CBDF. It does not refer to creating another exclusive political circle of cross-border data flow, but is regarded as a starting point to create new digital economic growth momentum for the benefit of countries around the world. China not only upholds the position of freedom, openness and win-win cooperation, but also welcomes any country that embraces the idea of a community with a shared future in cyberspace to join in. The legal framework for China's CBDF has just been established. The security assessment of outbound data transfers and the core system of this legal framework still need further improvements. As a consequence, the current channel of data flow abroad has not been completely opened up. With the further refinement and improvement of legislation, however, problems may be solved properly.

Received: November 1, 2023
Modified: February 15, 2024
Accepted: May 1, 2024

92 *Id.* at 41-2.