J. East Asia & Int'l L. Vol. 16/No.2 (2023); 267-282
Publication type : Research Article
Section : Issue Focus
DOI : http://dx.doi.org/10.14330/jeail.2023.16.2.04

China's Security Assessment Measures for Outbound Data Transfers

Junchao Liu*

Recently, China has published the "Security Assessment Measures for Outbound Data Transfers," a crucial regulation on outbound data flows. This regulation contains strong national security considerations and produces independent and direct legal effects compared with other assessment systems in China's laws. However, there is a possibility that conflict arises between these measures and the international commitments made by China due to the ambiguity in how "critical data" is defined, the excessive emphasis placed on self-risk assessment, and the arbitrary extension of procedures. Particularly, with China's current application to join the CPTPP, the restrictive measures of its cross-border data flow may appear to violate the obligation of CPTPP, but may be justified through CPTPP's exception clauses. In light of this, it is necessary for China to adopt a more modest approach to balancing data security with the effort made to promote the flow of cross-border data.

Keywords
Security Assessment, Outbound Data Transfers, Critical Data, Risk Self-Assessment, CPTPP

* Research Assistant at the Center for International Law of Cyberspace at Xiamen University's Law School. LL.M. (Xiamen). ORCID: https://orcid.org/0009-0008-3809-8126. The author may be contacted at 12920211154738@stu.xmu.edu.cn / Address: Xiamen University School of Law, No.422 South Siming Road, Xiamen 361005 P.R. China.
All the websites cited in this article were last visited on November 15, 2023.

I. Introduction

Since the new millennium, digital trade has expanded globally. According to a report released by the State Council of the People's Republic of China on the development of digital economy, China had signed the MoU on the cooperation with 16 countries in the "Digital Silk Road" by 2022, establishing bilateral cooperation mechanisms with 24 countries for "Digital Silk Road E-commerce."[1] As a result, the scale of China's cross-border e-commerce approached RMB 2 trillion in 2021.[2]

As a foundation of digital trade, the cross-border flow of data in China increases continuously, which is accompanied by a rapid growth in the demand for data compliance by enterprises. In this context, it is imperative to impose regulation on the cross-border flow of data in China for a balance to be reached between data security and the growth of digital economy. For this purpose, the Cyberspace Administration of China (CAC) officially published the "Security Assessment Measures for Outbound Data Transfers" (SAMODT) in September 2022, which marks the establishment of a critical management mechanism for the outbound flow of data based on security assessment.[3]

Notably, China attaches much significance to "national security"' and "data sovereignty" in the way that the outbound flow of data is regulated.[4] However, as a supporter of international governance in cross-border data flow, China sticks to a multilateral approach.[5] This is reflected by its possible exploration of joining global or regional digital trade rules systems. The active engagement of China in international digital governance is evidenced by its formal application to accede to the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP).[6] For a successful accession to the CPTPP, China needs to impose the

1 Lifeng He, Report on the Development of the Digital Economy, Chinese Government Portal [国务院关于数字经济发展情况的报告] (Oct. 28, 2022), https://www.gov.cn/xinwen/2022-11/28/content_5729249.htm.

2 *See In 2021, China's cross-border e-commerce imports and exports will reach nearly 2 trillion yuan* [2021年我国跨境电商进出口规模近2万亿元], Xinhuanet (Oct. 29, 2022), https://www.gov.cn/xinwen/2022-10/29/content_5722451.htm?eqid=e383f37b000dc1510000000464563959.

3 CAC, The Cyberspace Administration of China has answered questions about the "Measures for Security Assessment of Data Export" to journalist [《数据出境安全评估办法》答记者问] (July 7, 2022), http://www.cac.gov.cn/2022-07/07/c_1658811536800962.htm.

4 Ye Li, *Review and Improvement of China's Cross-Border Data Flow Rules under RCEP Agreement* [RCEP协定下我国数据跨境流动规则的检视与完善], 13(1) Sci. Tech. & L. [法律与科技（中英文）] 120-1 (2023).

5 Hai-jin Hao, *The International Soft Law Approach to Data Protection* [数据保护的国际软法之道], 39(2) Stud. L. & Bus. [法商研究] 166-70 (2022).

6 PRC Ministry of Commerce, China officially submits an application to join the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) [中方正式提出申请加入《全面与进步跨太平洋伙伴关系协定》

relevant CPTPP rules on its measures taken to regulate the cross-border flow of data, as represented by SAMODT, particularly the relevant provisions to its digital trade.

The paper aims to determine whether and how SAMODT can be effectively integrated with the rules governing the cross-border flow of data in the CPTPP. For this purpose, this paper outlines the primary restrictive measures of SAMODT on the outbound flow of data. Then, their compliance with the relevant CPTPP rules is assessed. Finally, the author will make the targeted recommendations to improve the transparency in China's regulation on outbound data flow and its digital economy.

II. Main Restrictive Measures in SAMODT

Article 1 of SAMODT provides that its legislative purpose is explicitly defined as "to ensure law-abiding and orderly free data flow." In practice, however, its primary objective is to regulate the outbound flow of data through a security assessment mechanism. For the greater effectiveness of this mechanism, the CAC released the "Guide to Applications for Security Assessment of Outbound Data Transfers (First Edition)" (hereinafter Guidelines), which is intended as a specific instructional manual for SAMODT.[7] In the Guidelines, the specific requirements are laid out with regard to the methods, procedures, and materials that must be submitted by the relevant entities when a security assessment is applied for. The Guidelines stipulate that the outbound flow of data must be deemed "necessary" as a prerequisite,[8] implying a conservative stance taken on the cross-border flow of data as a whole.

According to SAMODT, it is mandatory to conduct a security assessment in accordance with the law before "critical data" flows out of the country when such data is involved in cross-border data, the personal information processed by key information infrastructure operators, or the personal information exceeding the legal quantity threshold.[9] There are two fundamental principles outlined by SAMODT for the security assessment of outbound data flow. One is the combination of ex-ante assessment and continuous supervision. The other is the combination of self-risk

(CPTPP)] (Sept. 16, 2021), http://www.mofcom.gov.cn/article/xwfb/xwbldhd/202109/20210903199707.shtml.

7 CAC, Cyberspace Administration of China has released the Guidelines for the Application of Security Assessment for Cross-border Data Transfer (1st ed.) [国家互联网信息办公室发布《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.

8 Guidelines for the Application of Security Assessment for Cross-border Data Transfer (1st ed.), art. 2.

9 SAMODT art. 4.

assessment and government security assessment.[10] The former emphasizes that the security assessment is an ongoing process of evaluation, which requires continuous security monitoring. In this regard, continuous supervision is to monitor the changes in data protection capabilities, the fulfillment of obligations by data recipients, and the legal amendment made in the region where the data is received. The latter requires a dual evaluation of security. Following a self-risk assessment conducted by enterprises, a government security assessment is carried out.

Under this framework of security assessment, an observation can be made in the following areas regarding the restrictions on outbound data flow that are most likely to present challenges in the compliance with international rules.

A. Vaguely defined "Critical Data" as an Unexpectable Trigger Point

As mentioned above, a security assessment should be conducted on the cross-border data classified as "critical data." Thus, it is imperative to accurately determine the scope of critical data for both the law enforcement agencies and those entities involved in outbound data flow. According to Article 19 of SAMODT, "critical data" "may jeopardize national security, economic operations, social stability, public health and safety, among other factors if tampered with, destroyed, leaked, illegally obtained, or unlawfully used." To clarify the scope of critical data, it is necessary to take other relevant laws and regulations as reference.

Originally, the concept of "critical data" was raised in the Cybersecurity Law of the People's Republic of China (hereinafter Cybersecurity Law).[11] Subsequently, the Data Security Law of the People's Republic of China (hereinafter Data Security Law)[12] was published to mandate the establishment of a data classification and grade protection system by the state, providing different regions and departments with discretion in determining the specific catalogs of critical data. The Data Security Law emphasizes the focused protection of critical data. However, the definition of critical data varies by region without unified standards provided by the Data Security Law. Consequently, the practice of identifying critical data is constrained by uncertainty and inconsistency.[13]

To address this limitation, a series of guidelines have been published by the

10 *Id*. art. 3.

11 Cybersecurity Law arts. 21 & 37, http://www.cac.gov.cn/2016-11/07/c_1119867116.htm.

12 Data Security Law art. 21, http://www.cac.gov.cn/2021-06/11/c_1624994566919140.htm.

13 Xuewen Zhang, *The Rule of "Commercial Data Export": Ownership Analysis, Relationship Composition, Practical Orientation* ["商业数据出境"的规则之治：权属分析、关系构成、实践面向], 41(2) J. INTEL. [情报杂志] 176-88 (2022).

CAC and the National Information Security Standardization Technical Committee (NISSTC), *inter alia*, providing clarity on the scope, principles of identification, and verification methods for critical data. Among them, the "Guidelines for Identification of Important Data" (hereinafter Draft for Comments) provide a list of the main sectors where critical data is distributed, including government departments, key industry enterprises, public service institutions, authoritative professional institutions, research institutions, Internet companies, and real economy enterprises.[14]

Also, the Draft for Comments specifies the principles that apply to the identification of critical data, such as focusing on security impact, emphasizing key protection, ensuring the compliance with existing regulations, conducting thorough risk assessment, applying both quantitative and qualitative methods, carrying out dynamic identification and reevaluation, and specifying the attributes that critical data should possess.[15] Establishing standards for the threat posed by critical data to national security and public safety, the "Data Classification and Grading Guidelines" clarify that critical data excludes state secrets and the internal management information of enterprises.[16] However, these well-intentioned explanations lead to an overly broad scope of critical data, which makes them difficult to implement in practice.

As mentioned above, there remains no specific and highly operational standard established, despite the issuance of numerous laws and regulations from various angles in China as an attempt to define critical data. This results in a significant uncertainty in the identification of critical data. However, SAMODT sets out that any violation of its measures will be penalized in line with the Cybersecurity Law, the Data Security Law, the Personal Information Protection Law, and other applicable laws and regulations. In case that a crime is committed, criminal liability will be pursued according to the law. Due to a contrast between the vagueness of regulations by SAMODT and the high cost of illegal activities, both law enforcement agencies and data enterprises will take a cautious stance by classifying uncertain data as critical. Consequently, security assessment is triggered more frequently.[17]

14 Draft for Comments art. 5.

15 *Id.* art. 4.

16 Guidelines for Practice of Cybersecurity Standards - Network Data Classification and Grading Guidelines, art. 2.2.

17 XuKe, *Freedom and Security: China's Solution for Cross-border Data Flows* [自由与安全：数据跨境流动的中国方案], 34(1) Glob. L. Rev. [环球法律评论] 22-37 (2021).

B. Risk Self-Assessment Imposing Excessive Burden on Data Exporters

In China, the outbound transfer of data is subject to a regulatory framework under which the risk self-assessment by enterprises is combined with the security assessment conducted by the government.[18] In order to outline the key aspects of risk self-assessment, Article 5 of SAMODT makes it mandatory for data exporters to evaluate their data security capabilities and safety risks proactively. They are so required to submit their risk self-assessment report to the CAC prior to data transfer. This is effective in assigning greater responsibilities to enterprises in terms of data compliance. The content of the risk self-assessment is intricate and comprehensive, involving such factors as data volume, data types, data collection methods, processing frequency, export methods, the data security capabilities of data processors and recipients, and the legal documentation related to cross-border transmission. To meet these requirements, a wide range of professional skills and expertise are required.[19]

Field research data shows that there is a lack of understanding as to the importance of data export security among many companies in China; no internal control systems has been established yet to ensure data security compliance.[20] Additionally, China faces a shortage of professionals equipped with the specialist skills needed to comply with these requirements.[21] In this context, they are burdened with the mandate that data exporters must fully comply with the requirements of SAMODT and complete a risk self-assessment in advance.

Considering the actual declaration situation since the implementation of SAMODT, the disproportionate burden of risk self-assessment is evident to some extent. Following public information, the formal submission materials from just over 1000 companies have been received by the Cyberspace Administrations located in Beijing, Shanghai, Jiangsu, and Zhejiang.[22] This disparity between reality and

18 Wang Chun-hui, *Rules and Application of Data Security Exit Assessment-Interpretation of The Data Exit Security Assessment Measures* [数据安全出境评估规则与适用], 24(4) J. Nanjing U. Posts & Telecomm. (Soc. Scl.) [南京邮电大学学报（社会科学版）] 1 (2022).

19 Zhong Yan Law Office, Key Points and Practical Issues of Data Export Routes [数据出境路径要点与实操问题] (July 7, 2023), http://www.zylawoffice.cn/nd.jsp?id=212.

20 *See* Global Law Office, Survey and Analysis Report on Data Cross-Border Status quo - Basic Issues and Solutions to Ten Pain Points (2023), at 15-30, http://www.glo.com.cn/UpLoadFile/Files/2023/3/2/135336162dd926879-c.pdf.

21 Zhonglu Zeng & Ke Li, *Detecting Weak Signals Based on Companies' Annual Reports: A Study of Future Trends in Demand for Compliance Talents* [基于公司年报的弱信号发现：未来合规人才需求趋势研究], 46(4) Info. Stud.: Theory & Application [情报理论与研究] 8-14 (2023).

22 All Bright Law Office, Analysis of the Trend and Successful Cases of Enterprise Data Export Declaration [企业数据出境申报趋势与成功案例分析] (July 25, 2023), https://www.allbrightlaw.com/CN/10475/78240f86a770dd63.aspx.

expectations highlights that many enterprises remain hesitant and observant rather than proactive.

C. Lengthy Procedures Only Yielding a Superficial Assessment Report

Among the companies that have submitted applications for security assessments, only 15 have passed it, which means a pass rate of just one percent.[23] This is attributable to two reasons.

On the one hand, the Guidelines define the division of responsibilities and workflow between local Cyberspace Administrations and the CAC during the declaration stage.[24] Local agencies are assigned the responsibility to receive declaration materials and conduct a completeness check, despite no need to decide on whether to accept the application (formal review). If the application from data exporter passes the formal review, the declaration materials are then forwarded to the CAC, which makes the final decision on whether to accept the application. In addition to the formal review, however, local agencies are required in practice to assess the 'legality,' 'necessity,' and 'justifiability' of cross-border data transfer.[25] They are also responsible for overall supervision on the process of data transfer. The lack of professional personnel and technical capabilities makes it difficult for local agencies to monitor the entire process of cross-border data flow in real time. To prevent overseas data leakage, they are often inclined to impose high standards on data security assessments and to reject some applications that might have otherwise passed the formal review.

On the other, the process of verification and cross-checking is required to be more detailed during the review of materials, as mentioned earlier. For instance, the Guidelines mandate companies to comprehensively describe the export chain in their self-assessment report, including the details about the provider of each chain, the number of chains, bandwidth, and IP addresses.[26] Throughout the process, it is possible that the materials are required by both local agencies and the CAC to be modified and improved repeatedly. The substantive review process of the CAC can last longer than 45 working days in many cases. Given the current progress announcements regarding security assessment work, the assessment lasts much

23 *Id*. at ¶ 2.

24 Guidelines art. 2.

25 Haoyu Jiang, *Research on the Confirmation of the Legality of the Financial Data Cross-Border Transferring Behavior* [金融数据出境行为的合法性认定研究], 40(2) Credit Reference [征信] 4-9 (2022).

26 Guidelines, attachment 2 & 4, at 8-16, https://www.tc260.org.cn/upload/2022-09-01/1661994372338082993.pdf.

longer than 57 working days in practice, which is even true for the first batch of companies completing their declarations. These lengthy procedures severely hinder the rapid development of digital economy.[27]

III. Prima Facie Violation and Justification under CPTPP

As a typical American digital trade rule, the CPTPP requires the contracting parties to promote the cross-border flow of data to the greatest extent possible while reducing local data storage.[28] Chapter 14 of the CPTPP is dedicated to addressing the rules related to e-commerce. Article 14.11 outlines cross-border data transfer in the three paragraphs which:

1. confirms the regulatory authority of the contracting parties over the cross-border flow of data;
2. imposes binding obligations on the contracting countries to limit those measures causing hindrance to the cross-border flow of data; and
3. permits legitimate justifications for the measures that might constitute violation of the second provision otherwise.

If the measure taken by a contracting country is found to contravene Article 14.11(2) and cannot be justified under Article 14.11(3), it possibly remains legitimate under the security exception clause in Article 29.2. In this regard, the author will evaluate whether the data export restrictions imposed by SAMODT are compliant with the relevant provisions of the CPTPP under this framework.

A. Prima Facie Violation of Article 14.11(2)

As the central provision on cross-border data flows, Article 14.11(2) of the CPTPP stipulates that "Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person."[29] In this provision, the term "shall

27 *Id*. *See also* Jun He Law Office, How to Handle the Security Assessment of Data Export [企业如何办理数据出境安全评估—《数据出境安全评估办法》正式发布] (Aug. 20, 2022), https://www.junhe.com/legal-updates/1858.

28 Nan-xiang Sun, *CPTPP Digital Trade Rules: Institutional Competition, Regulatory Differences, and China's Responses* [CPTPP数字贸易规则：制度博弈, 规范差异与中国因应], 45(5) Acad. F. [学术论坛] 44-52 (2022).

29 CPTPP art. 14.11(2).

permit" is invoked to impose a mandatory obligation on the contracting parties. Notably, such an obligation is restricted to the commercial activities conducted by "covered persons."[30]

At present, the security assessment of outbound data transfer is the primary measure taken by China to gain control on data exports. It applies to all scenarios of data export except when data is collected for law enforcement or judicial purposes. Therefore, those cross-border data transfers due to the commercial activities of "covered persons" are encompassed. However, the contracting parties are mandated by Article 14.11(2) to ensure that there are no restrictive conditions imposed on the cross-border transfer of information via electronic means. In essence, it is possible that a substantive restriction on China's data exports is constituted by the uncertainties caused by the security assessment, the high burden of risk self-assessment, and the protracted procedures, which could result in a technical violation of the CPTPP obligations.

Moreover, given the growing demand for outbound data transfer in China, data export can be further constrained by the specific process of implementing SAMODT. In particular, the result of security assessment is valid for only two years, and data exporters would be required to reapply for assessment if it changes during this period to the legal environment within the jurisdiction of the recipient. This increases its complexity, thereby hindering cross-border data transfer.

B. Justification under Article 14.11(3)

If the measures outlined in SAMODT constitute a breach of Article 14.11(2) of the CPTPP, legitimate justification may be sought under the exception clause specified in Article 14.11(3). However, three conditions below should be met simultaneously as follows:

1. The measure is intended to achieve a "legitimate public policy objective";
2. It involves neither arbitrary or unjustifiable discrimination nor disguised trade restrictions; and
3. It does not exceed what is considered necessary to achieve the intended policy objective.[31]

30 The scope of "covered persons" in the CPTPP is derived from the Trans-Pacific Partnership (TPP) and does not include "financial institutions" or "cross-border financial service providers of a party." The reason for this is that during the global financial crisis in 2008, the US banking regulators had difficulty accessing offshore data held by US banks. *See* Jinxia Shi, *The Key Issues in the Negotiations on China's Accession to the CPTPP* [中国加入CPTPP谈判中的服务贸易重点问题], 35(4) Peking U. L. J. [中外法学] 845-64 (2023).

31 European Commission, Questions & Answers on the Adoption of the Adequacy Decision Ensuring Safe Date Flows

That is to say, any measure taken under SAMODT to impose restriction on cross-border data flows out of China must meet these three conditions to be justified under the framework of the CPTPP. The following are the criteria to evaluate the three conditions.

1. Whether the restrictions of SAMODT on data outbound transfers are sufficient to achieve "legitimate public policy objectives"?

Despite no specific definition given out in Article 14.11 of the CPTPP as to the scope of "legitimate public policy objectives," Article 29.1, paragraph 3 stipulates: "For the purposes of Chapter 14 (Electronic Commerce), paragraphs (a), (b) and (c) of Article 14 of GATS are incorporated into and made part of this Agreement." In accordance with Article 14 of GATS, the public policy objectives that can be invoked as "exceptions" are listed in detail, including the measures required to protect "public morals" or maintain "public order," and the measures considered necessary to "protect human, animal, or plant life or health."

As confirmed by the Panel of Experts in the *US-Gambling* case, when Article 14 of GATS is interpreted, "public morals" refer to "the standards of right and wrong conduct maintained by or on behalf of a community or nation," while "public order" refers to "the preservation of the fundamental interests of a society, as reflected in public policy and law."[32] These fundamental interests can relate, *inter alia*, to standards of law, security, and morality."[33] In fact, despite the different concepts represented by "public morals" and "public order," their common purpose is to uphold the public interest. It is thus unrealistic to separate them completely, because both of them can evolve and change with societal development.[34] As a leader in formulating rules for cross-border data flow, the US has interpreted the legitimate public policy objectives in its free trade agreements and government work reports, such as public morality, national security, and personal data protection.[35] Cybersecurity is also included as a general exception in the WTO Electronic

between the EU and the Republic of Korea (Dec. 17, 2021), https://ec.europa.eu/commission/presscorner/detail/en / qanda_21_6916.

32 Panel Report, *United States-Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WTO Doc. WT/DS285/R (adopted Apr. 20, 2005), https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S006.aspx?DataSource=Cat&query=@Symbol=WT/DS285/R&Language=English&Context=ScriptedSearches&languageUIChanged=true.

33 *Id*. at 467.

34 *Id*. at 461.

35 Xu Li, *"Exceptions to legitimate public policy objectives" in cross-border data flow regulation and China's practice* [跨境数据流动规制之"合法公共政策目标例外"与中国实践], 4 Seeker [求索] 154-67 (2023).

Commerce Consolidated Negotiating Text.[36]

According to SAMODT, only those entities closely related to cybersecurity are either subject to a security assessment of outbound data transfer, such as the operators of critical information infrastructure, or the subjects related to privacy and digital rights, particularly when the outbound data carries critical data or a large amount of personal information or sensitive personal information.[37] As stated above, the restrictions imposed by SAMODT on outbound data transfer are purposed to uphold cybersecurity, important public interests, or personal privacy. In addition, they should be considered as legitimate public policy objectives as laid down in Article 14.11(3).

2. Whether the restrictions imposed by SAMODT on outbound data transfer constitute arbitrary or unjustified discrimination or disguised trade restrictions?

In order to prevent the exception clause from being abused, the same wording as the introductory part of Article 20 of the GATT is adopted in the CPTPP. To ascertain whether a measure constitutes arbitrary or unjustified discrimination or disguised trade restrictions, there are four elements to be aligned. Firstly, a discriminatory outcome must result from the application of the measure. Secondly, the discrimination must be arbitrary or unjust in nature. Thirdly, the discrimination must be occurred in the countries under similar conditions. Lastly, disguised trade restrictions must be interpreted as 'concealed' or 'unannounced' restrictions. [38]

In accordance with SAMODT, the CAC is responsible for uniformly organizing and implementing the security assessment, and setting out the clear procedures, content, standards, etc. The security assessment applies equally to eligible entities. In this regard, a full right to know is ensured by the transparency of its implementation. It can be inferred that there are no arbitrary, discriminatory, or disguised trade restrictions when the CAC is assumed to follow the security assessment procedures and standards strictly.[39]

Given that two-thirds of the enterprises are foreign companies,[40] the security

36 *See WTO Electronic Commerce Consolidated Negotiating Text*, World Trade Online (Oct. 26, 2020), https://insidetrade.com/trade/wto-e-commerce-negotiators-aim-end-year-consolidated-text.

37 SAMODT art. 4.

38 Appellate Body Report, *United States-Import Prohibition of Certain Shrimp and Shrimp Products*, WTO Doc. WT/DS58/AB/R (adopted Oct. 12, 1998), https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=58544&CurrentCatalogueIdIndex=0&FullTextSearch=.

39 Chen-jin Xu, *China's Legal Framework on Cross-border Data Flow and its Compliance with the CPTPP Requirements* [中国跨境数据流动规制体系的CPTPP合规性研究], 39(2) Int'l Econ. & Trade Res. [国际经贸探索] 69-82 (2023).

40 *Id*. at 22.

assessment should be designed specifically for outbound data transfer, thereby increasing operating costs for foreign enterprises and constituting arbitrary, unjust discrimination and disguised trade restrictions. The author would argue as follows. Firstly, the risk posed by outbound data transfer is truly higher, which requires special regulations. Secondly, according to Article 32 of the Regulations on the Administration of Network Data Security (Draft for Comments), a security assessment must be conducted at the time of sharing, trading, or entrusting the processing of important data within China. Also, its content is not starkly different from the security assessment of cross-border data flow. Finally, there are openness and transparency in the security assessment process. Even though restrictions may be imposed on overseas data recipients, these restrictive measures are transparent and justifiable. The execution of security assessments should not be considered discriminatory or impose trade restrictions on overseas data recipients, as long as there are no unreasonable requirements specifically targeting overseas entities.[41]

3. Whether the restrictions imposed by SAMODT on outbound data transfer exceed the necessary limits?

As required by the application of this element, measures are subject to the "necessity test," which can be derived reasonably from Article 20 of the GATT. In the *Korea-Various Measures on Beef* case, the Appellate Body reports that "necessity" means the measure taken to achieve a goal and it should be exceedingly close to the limit of being 'indispensable.'[42] A measure cannot be considered necessary if it contributes only to the achievement without meeting the criteria of the "necessity test."[43] In general, a measure is considered 'necessary' only when no reasonably available alternative measures are less trade-restrictive. Three conditions required for the "necessity" requirement in the Appellate Body Report of the *US-Gambling* case are as follows: (1) the significance of the benefits and value brought by the measures; (2) the contribution of the measures to the achievement of the objectives; and (3)the restrictive impact made by the measures on international trade.[44]

On this ground, it is arguable that SAMODT would fail the "necessity test." Also, the existence of alternative solutions must be demonstrated that can also achieve specific public policy objectives but with fewer trade restrictions imposed. In this

41 *Supra* note 36.

42 Appellate Body Report, *Korea-Various Measures on Beef*, WTO Doc. WT/DS161&169/AB/R (adopted Jan. 10, 2001).

43 *Id.* at 161.

44 Panel Report, *supra* note 32, at 306.

aspect, it is possible to examine those foreign measures with the similar purposes to SAMODT. In line with the GDPR and the Regulation on a Framework for the Free Flow of Non-personal Data in the European Union, the EU takes measures to restrict the cross-border flow of data through an "Adequacy Decision."[45]

In essence, this decision is similar to security assessment. Article 45 of the GDPR provides the EU has the authority to assess and continuously monitor the level of data protection in those countries outside its territory. When the Commission determines that there is a level of data protection equivalent to that of the EU provided by a country, a specific region or industry of a country, or an international organization, the data transfers to such entities is permitted.[46] As stipulated in Article 45, paragraph 3, the EU should review the level of data protection in these countries at least once every four years. As for China, its security assessment is similar to the EU's "Adequacy Decision" in content, without provisions imposed on the data recipient to meet the requirement of "equal protection."[47] Therefore, China's security assessment is arguably less restrictive for cross-border data transfer.

In the US, there is not yet dedicated supervision system established for cross-border data flow. However, rigorously supervision applies to the data deemed important through export control and foreign investment security review. For example, when ByteDance (TikTok's parent company) was banned by the Committee on Foreign Investment in the United States (CFIUS) from the access to US user data, TikTok was required to transfer all data of the American users to Oracle's servers in the US, which is due to national security concerns. the US review standards represent a stricter, more trade-restrictive supervision mechanism than the measures of SAMODT. Therefore, the security assessment arguably has minimal impact on the restriction of data outbound transfer, if China's national security interests are protected.

C. Justification under Article 29.2 of CPTPP

Even though invoking Article 14.11(3) of CPTPP fails to legitimize the restrictions imposed by SAMODT on cross-border data flow, it is still possible to legitimize

45 European Commission, Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN.

46 Jin Jin, *EU rules, global standards? "Competition for the top" of cross-border data flow regulation* [欧盟的规则，全球的标准？数据跨境流动监管的"逐顶竞争"], 35(1) Peking U. L. J. [中外法学] 46-64 (2023).

47 Liu Ye, *The Selection of GDPR's Dual Protection Modes of Cross-Border Data Transmission* [论GDPR数据跨境传输二元保护模式的选择], 3 J. Int'l Econ. L. [国际经济法学刊] 16-30 (2023).

them by invoking Article 29.2 of CPTPP (Security Exceptions), which provides: "nothing in CPTPP shall be construed to preclude a Party from applying measures that it considers necessary for the fulfillment of its obligations with respect to the maintenance or restoration of international peace or security or the protection of its own essential security interests." [48] As interpreted in the panel report of *Russia - Traffic in Transit*, there are three requirements to satisfy before the "Security Exceptions" apply.[49] First, the members are entitled to define what their fundamental security interests are and decide which measures are necessary. Second, the members must adhere to the principle of good faith when their basic security interests are defined. Lastly, a minimum level of reasonableness must be reached by the measures implemented.[50]

"Security exceptions" exclude the security benefits solely based on commercial purposes. Therefore, two burdens of proof arise from invoking Article 29.2. On the one hand, it must be clarified what kind of "security interests" are guaranteed by the security assessment of outbound data transfer. On the other hand, it must be demonstrated that there is a "minimum reasonable" correlation present between the measure and "security interests." [51] In addition, the scope of "security interests" has been expanded under the context of intensified geopolitical competition from the traditional military domain to other areas such as climate change, cybersecurity, the coronavirus pandemic, as well as food and energy security.

As stipulated in Article 1 of SAMODT, its legislation is aimed "to regulate outbound data transfers, protect personal information rights and interests, safeguard national security and social and public interests." It can be seen that the interests protected by the security assessment of outbound data transfers can be covered by "security interests." The subject of security assessment is confined to critical data, the personal information generated by critical information infrastructure, or large-scale personal information. As for China, a leak of the above data abroad can pose a huge threat to its national security. Therefore, security assessment is significant, showing a "minimum reasonable" correlation with "security interests." The basic requirements of Article 29.2 can be invoked and met, as long as China conducts the security assessment of outbound data transfer in "good faith," refrains from arbitrarily expanding the scope of application, or pursue trade interests under the condition of

48 CPTPP art. 29.2.

49 Panel Report, *Russia-Measures Concerning Traffic in Transit*, WTO Doc. WT/DS512/R (adopted Apr. 5, 2019), https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds512_e.htm.

50 *Id.* at 5-6.

51 *Id.* at 138.

security.[52]

IV. Lessons

While the restrictive measures in SAMODT against cross-border data flow are suspected to breach the obligations of CPTPP, they may be legitimized in accordance with the exception clause. However, it is difficult to successfully invoke the exception clause in Free Trade Agreements (FTA) because negotiation requires high cost.[53] To achieve alignment between SAMODT and CPTPP, we cannot rely solely on the exception clause.

A. Clarifying the Concept and Coverage of Critical Data

It is necessary to comply with the concept of legislative compliance and the orderly free flow of data. This purpose can be achieved by narrowing down the scope of critical data through a "negative list."[54] Also, a "whitelist system" for cross-border data flow must be established by creating an inclusive and accommodating legal environment for various innovative fields, such as cross-border use of AI technology and data supervision sandboxes, with an appropriate degree of review exemption granted to the outbound transfer of data within these industries.[55] In line with the PRC Digital Security Law, the standards for compiling critical data catalogues can be unified to eliminate the barriers to the flow of commercial personal information, while lowering operating costs for enterprises.

B. Improving the Rationality of Risk Self-Assessment

As a professional and cost-intensive process, risk self-assessment requires enterprises to identify the scope of exported data effectively, control and supervise the paths and interfaces of outbound data transfer continuously, and achieve compliance

52 Shi-xi Huang, *Data Localization Regulations and Security Exception Defenses in CPTPP* [CPTPP中的数据本地化规制与安全例外抗辩],11 Intertrade [国际贸易] 81-7 (2022).

53 Bo He, *Challenges and Countermeasures for China's Participation in International Rules of the Cross-border Data Flows* [中国参与数据跨境流动国际规则的挑战与因应], 4 Admin. L. Rev. [行政法学研究] 89-101 (2022).

54 Jin-rui Liu, *Towards Global Regulation of Cross-Border Data Flows: Fundamental Concerns and the Chinese Approach* [迈向数据跨境流动的全球规制：基本关切与中国方案], 4 Admin. L. Rev. [行政法学研究] 73-86 (2022).

55 Xiao-ning Pan, *Thoughts on Improve the Cross-Border Transfer of Personal Information Data in China* [完善我国个人信息数据出境制度的思考], 40(6) J. Customs & Trade [海关与经贸研究] 81-92 (2019).

management.[56] According to the Guidelines, enterprises are required to evaluate the "legality," "necessity," and "justifiability" of outbound data transfer. This overlaps with the work of the CAC. To reduce the burden imposed on enterprises and enhance their enthusiasm for the security assessments of outbound data transfer, it is advisable to entrust the responsibility for assessing legality to the local Cyberspace Administration. While for enterprises, they can focus attention on the assessment of "justifiability" and "necessity."

V. Conclusion

There has been a trend of fragmentation shown by the rules of global cross-border data transfer due to a range of external factors such as the variations in legal cultures, institutional backgrounds, and economic conditions. Nevertheless, it is a universally recognized idea of promoting the cross-border flow of data. China, as the world's largest developing country, is responsible for leading the rest of the world in formulating global digital economic rules and upholding the interests of developing nations. Aside from demonstrating its sincerity and interest in international cooperation for digital economy, the application of China to join CPTPP also underscores its open and inclusive approach to digital governance. By seeking membership in the CPTPP negotiations, China aims to participate in discussing data governance; expand the global influence with its rules and ideas; and contribute its solutions to the global regulation of cross-border data flow.

Received: August 1, 2023
Modified: September 15, 2023
Accepted: November 1, 2023

56 Tong Chen, *The Understanding and Application of Risk Self-Assessment Mechanism for data outbound transfer* [数据出境风险自评估机制的理解与适用], 4 Enter. Econ. [企业经济] 144-51 (2023).