THE LEGAL FRAMEWORK FOR CROSS-BORDER DATA TRANSFER BETWEEN MAINLAND CHINA AND HKSAR

Junxuan Wu*

Abstract: Cross-border data transfer is a hard issue in today's world of "digital nationalism". In this post-Snowden world, data-localization has become the norm. China has adopted data localization rules in various laws, from Internet Security Law to Data Security Law. China's constitutional structure of "one country, two systems" presents a unique question to data localization: should cross-border data transfer between the Mainland and SARs (Special Administrative Regions) be constrained by data-localization rules? Since both basic laws for Hong Kong and Macau define these two SARs as "free trade" zones and "separate customs" territories, once data from the Mainland are transferred to the SARs, there would be no existing laws to hinder their further flow to the globe. Furthermore, the SARs have their laws protecting data rights and regulating data use, which are quite different from the national laws. These unique features render cross-border data transfer *within* China a challenging and interesting topic. This article takes the challenge by focusing on the legal framework for data transfer between Mainland China and Hong Kong. It delineates the relevant legal rules in China and its HKSAR, points out the obstacles and difficulties, and suggests reforms.

Keywords: Cross-Border Data Transfer, Digital Sovereignty, Data Localization, National Security, Hong Kong SAR, Mainland China

* KoGuan Law School, Shanghai Jiao Tong University, China.

Table of Contents

INTRODUCTION

It is often believed that the Internet is borderless and data flow is free. However, this belief is untrue from both technical and legal perspectives. Technically, data flow is controlled by border gateway protocol and firewalls. Legally, it is regulated by data transfer rules. Actually, tightening border control on Internet is the general trend in the whole world except in the United States, because the U.S. Internet hegemony is the reason for all other countries to defend their digital border by making data localization rules. Anupam Chander called this trend "data nationalism" and made a general description: "The era of a global Internet may be passing. Governments across the world are putting up barriers to the free flow of information across borders. Driven by concerns over privacy, security, surveillance, and law enforcement, governments are erecting borders in cyberspace, breaking apart the World Wide Web. The first generation of Internet border controls sought to keep information out of a country-from Nazi paraphernalia to copyright infringing material.' The new generation of Internet border controls seeks not to keep information out but rather to keep data in. Where the first generation was relatively narrow in the information excluded, the new generation seeks to keep all data about individuals within a country."[1333]

On the other hand, data flow is gradually surpassing traditional cross-border trade of goods and investment, becoming a new driving force for global economic growth. Today, with the vigorous development of the digital economy, cross-border data activities are becoming more and more frequent, and the demand for data outbound transfer by data processors is growing rapidly. Major countries and regions in the world have made various bilateral and multilateral legal arrangements to facilitate cross-border data transfer and used "adequacy" standard to make sure that data trading partners have laws adequate to protect personal information rights and interests.[1334] Legal tools such as TIA (Transfer Impact Assessment) have been developed to address the issue of balancing data trade and data security.

As a major digital economy country, China especially needs to promote cross-border data flow. On the other hand, given the current situation of U.S.-China relationship, China also needs to make sure that its outbound data flow should not undermine its national security and citizen's personal information rights. Since the listing of "Didi Chuxing" in the United States was urgently suspended,[1335] it is no longer feasible for companies to list in the United States due to national data security considerations; on the other hand, due to the mainland's favorable attitude towards listing in Hong Kong, attracted Didi and other data-related companies to turn their attention to Hong Kong, and consider listing in Hong Kong as the main way to obtain global investment. A large number of companies are listed in Hong Kong, and huge amounts of data and information flow seamlessly between the two regions every day, which brings about the legal issues of cross-border data flow between mainland China and Hong Kong. The Hong Kong Special Administrative Region and the Mainland are in different legal jurisdictions, and the flow of data between the two places constitutes cross-border flow. However, current academic research mainly focuses on the study of

---

[1333] Chander, A. and Le, U. P. (2015), Data Nationalism. *Emory Law Journal*, 64(3), 677-740.
[1334] Taylor, Mistale (2023). *Transatlantic Jurisdictional Conflicts in Data Protection Law: Fundamental Rights, Privacy and Extraterritoriality*. Cambridge University Press. 193-195.
[1335] Zhang, Angela Huyue (2024). *High Wire: How China Regulates Big Tech and Governs Its Economy*. Oxford University Press. 57.

cross-border data flow between different countries. Regarding the flow of data between Mainland China and Hong Kong HKSAR, two jurisdictions within one country, there is almost no academic research. This paper intends to fill in the gap.

It starts from a general description of the laws and regulations regarding data of the two places themselves, sorts out and analyzes their regulations and restrictions on data exports, including China's legal control of mainland data retrieval, then compares their regulatory thresholds, regulatory intensity, regulatory purposes, etc.. Next, it identifies the practical problems in cross-border flows from mainland China to the Hong Kong Special Administrative Region. Finally, it proposes certain reforms to address these problems.

I. Mainland China's Regulations and Restrictions on Cross-border Data Transfer

A. Definition of Data Export

1. Definition of Data

To clarify what "data transfer" is, we first need to clarify what data is. Regarding the definition of data, academic circles have given many opinions from different angles, such as "an information carrier designed to record the subjective reflection of the subject of knowledge on the object of knowledge" and "information is the expression of knowledge and the reaction of the human brain to data. Data is "the embodiment of information" "massive, high-growth and diversified information assets" and so on. EU Database Directive defines data as "any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording." However, these definitions are all derived from papers published before 2021. Since there has been a clear definition of data in specific laws, it is proper for this article to adopt legal definitions. According to Article 3 of the "Data Security Law of the People's Republic of China" (hereinafter referred to as DSA), data is "any record of information in electronic or other forms." This legal definition gives data a very broad scope, and any record of information electronically or otherwise can be considered data. It is worth noting that data can be divided into many types from different perspectives. For example, based on the subject or purpose, it can be divided into "personal data, business data, technical data, and organizational (public) data". Different types of data, when transferring cross border, may bring about different kinds of legal issues, from privacy, trade secrets to national security. Article 21 of DSA provides that "the state establishes a data classification and hierarchical protection system, and implements classified and hierarchical protection of data according to the importance of data in economic and social development." It suggests that different data, according to their different social values, shall enjoy different levels of protection and regulation. To implement the classification-based and hierarchical regulatory system, detailed regulations have been made.

2. Two Definitions of Cross-Border Data Transfer

Among several existing studies on cross-border data flows, there are two main

mainstream definitions of data export. The first definition is taken from an article published by the United Nations Center on Transnational Corporations in 1984, which defines "Cross-border data flow" as the situation in which "electronic information records generated in one country are read, stored, used or processed by private entities or public authorities in other countries".[1336] This definition emphasized the "transnational" nature of cross-border data transfer.[1337] However, in China's "One Country, Two Systems" constitutional order, there are borders within one country. Hong Kong and Macau, as China's Special Administrative Regions established in accordance with Article 31 of the Constitution, maintain their unique legal systems. Therefore, data transfer between the Mainland and the two SARs should be considered as "cross-border" data transfer. Therefore, "cross-border data transfer" should be redefined as "data generated in one jurisdiction are processed by persons and entities in other jurisdiction(s)".

This definition is not clearly expressed in relevant laws and regulations in China. For example, the Guidelines for Data Export Security Review defines data export as "a one-time or continuous activity in which a network operator provides personal information and important data collected and generated during its operations within the territory of the People's Republic of China to institutions, organizations or individuals outside the country through the Internet or other means, by directly providing or conducting business, providing services or products, etc." Here, "export" means leaving "the territory of the People's Republic of China". A literal reading of this definition may lead to the conclusion that data transfer between Mainland China and HKSAR doesn't constitute data export, because data is still within the territory of China. This kind of confusion is quite common among foreign observers of Chinese law. For example, while discussing the four conditions imposed by the Personal Information Protection Law (PIPL) on cross-border transfer of personal information, Graham Greenleaf cautioned: "It is possible but uncertain that this prohibition might also include Hong Kong."[1338] For any Chinese lawyer, this kind of uncertainty doesn't exist. Legal rules are located in a system of laws under a Constitution. Systematic interpretation of specific rules solves such uncertainty. Article 31 of the Constitution authorizes the National People's Congress (NPC) to establish Special Administrative Regions and their applicable laws. The Basic Law of the Hong Kong Special Administrative Region of the People's Republic of China (hereinafter referred to as the "Basic Law") is a law passed by the NPC and applied to Hong Kong. The Basic Law makes sure that Hong Kong not only enjoys a high degree of autonomy, but also implements laws that are different from those in mainland China. Within such a unique constitutional framework called "One Country, Two Systems", a range of laws, from immigration and border control laws to trade-related laws, established borders between the Mainland and Hong Kong. For example, Article 89 of the Border Exit and Entry Administration Law (《出入境管理法》) defines border exit (出境) as traveling from the mainland of China to other countries or regions, including traveling from the mainland of China to the Hong Kong Special Administrative Region. Obviously, if the traveling of natural persons from the mainland to Hong Kong is crossing the border, traveling of data from mainland

[1336] UNCTC. Transnational Corporations and Transborder Data Flows. The United Nations, 1984.
[1337] Arner, Douglas W., Castellano, Giuliano G., & Selga, Eriks. The Transnational Data Governance Problem. *Berkeley Technology Law Journal*, 2021, 37(2): 623-699.
[1338] Greenleaf, Graham. Personal Data Localization and Sovereignty along Asia's New Silk Roads. In Chander, Anupam, & Sun, Haochen (eds.), *Data Sovereignty: From the Digital Silk Road to the Return of the State*. Oxford University Press, 2023. 301.

to Hong Kong should also be considered as cross-border transfer. Therefore, the conditions imposed by Article 38 of PIPL on cross-border data transfer clearly apply to mainland China-Hong Kong data transfer, including (1) Passing a security assessment organized by Cyberspace Administration of China (CAC) following the provisions of Article 40 of PIPL; (2) Obtaining personal information protection certification through a professional institution; (3) Entering into a standard contract (formulated by CAC) with the overseas recipient, stipulating the rights and obligations of both parties; (4) Other conditions prescribed by laws, administrative regulations or CAC rules.

B. Development of Legislations and Regulations on Cross-border Data Transfer in China

1. Early Data Export Legislation and Characteristics

Article 59 of the National Security Law is the earliest law regarding the security supervision of data exports, but it does not specifically mention data export. This article believes that the characteristics of mainland China's early cross-border data transfer laws can be characterized as low-level, fragmented, narrow coverage, weak operability, and low flow permission. First, the level of the rules is low. There is no national laws to stipulate rules on data transfer. The most high-level rules before the "13th Five-Year Plan" are only administrative regulations in nature, followed by "notices" in the rank of “other normative documents", national standards, and even non-standard documents. It has a mandatory effect and the legislative level is generally low. Second, fragmentation is caused by low rank, because the unity of law is achieved in China by a hierarchical structure stipulated in the Law on Legislation with the Constitution on the top. Fragmentation is reflected in the fact that the regulations on the export of different types of data are scattered in different notices, regulations, and technical documents. For example, the outflow of personal financial information is regulated by the "Notice of the People's Bank of China on Banking Financial Institutions Good Practices in Protecting Personal Financial Information", while the data held by credit reporting agencies is regulated by the "Regulations on the Administration of the Credit Reporting Industry". Because a single document cannot regulate all data exports, there are situations where different documents regulate different special fields. Moreover, these documents are concentrated in the special fields of financial and transportation credit reporting and are narrow in scope and not comprehensive enough. Third, weak operability and low mobility permissions are reflected in the fact that most of the regulations are broad rough, sometimes simply stipulate that data "should be within the country" and "should not be provided overseas". There is a very obvious tendency for data to be stored locally, even if there are exceptions. In situations such as "unless otherwise provided" and "statutory permission", these exceptions have not been specifically refined.

2. The Gradual Formation and Preliminary Improvement of Data Export Legislations

In 2016, the State Council issued the "Thirteenth Five-Year Plan for National Informatization", which clearly stated the strategic requirement of "establishing a security supervision system for cross-border data flows." Since then, legislative supervision of data exports has been gradually and systematically established and

improved. In November 2016, the "Cybersecurity Law of the People's Republic of China" (hereinafter referred to as the "Cybersecurity Law") was promulgated, and the provisions of Article 37 reflect the requirements for data localization. Data can only be exported abroad if it is truly necessary to provide it overseas and if it passes the security assessment. The Cybersecurity Law establishes for the first time in law a security assessment system for the outbound transfer of personal information and important data of critical information infrastructure operators and authorizes the national cybersecurity and informatization department to work with other regulatory authorities to formulate detailed security assessment implementation measures. In April 2017, the "Measures for Security Assessment of Personal Information and Important Data Transfer Abroad (Draft for Comments)" was released, establishing a basic framework for data transfer abroad. Subsequently, the "Data Transfer Security Assessment Guidelines (Draft)" and "Data Transfer Security Assessment Guidelines (Draft for Comments)" further specified the framework, clarified the concepts, and refined the security assessment process. In June 2019, the Cyberspace Administration of China released the "Measures for Security Assessment of Personal Information Transfer Abroad (Draft for Comments)", which details the assessment process for the transfer of personal information abroad to ensure the security of personal information in cross-border data flows.

It is worth noting that at this time, the regulations and national standards of various departments are mostly formulated based on the Cybersecurity Law, and some are formulated based on the National Security Law. However, at this time, China's data export regulations are largely departmental implemental rules detailing the above-mentioned laws. There is no high-level law to guide the system.

3. Attitude Changes and Three Pillars of Data Export Legislation

2021 is the year when data export legislation will be more perfect, and it will also be the year when the regulatory attitude in legislation shifts from data localization to a balance between data protection and utilization. In April, the State Council executive meeting passed the "Critical Information Infrastructure Security Protection Regulations" as administrative regulations. In June, the Data Security Law came into being. In this law, the legislative purpose is eye-catching. Among them, the legislative purpose of "promoting data development and utilization" appears for the first time, and precedes the statement of "protecting the legitimate rights and interests of individuals and organizations", implying that the country's regulatory attitude towards data export has begun to change, and it recognizes the importance of data development and utilization. Where necessity and value lie, the balance is quietly tilting from data localization to the orderly and free flow of data by the law. Article 3, Paragraph 3 of the "Data Security Law" directly states that it is necessary to ensure that data is in a state of effective protection and legal use, emphasizing the balance between protection and use. In August, the Standing Committee of the 13th National People's Congress passed the "Personal Information Protection Law", which provides a special chapter on cross-border rules for personal information and also mentions "promoting the reasonable use of personal information" in the legislative purpose. At the end of October, the Cyberspace Administration of China released the "Measures for Security Assessment of Data Transfer Abroad (Draft for Comments)", which further reflects the regulatory tendency of the free flow of data by the law. In November, the Cyberspace Administration of China issued the "Regulations on the Management of Network Data

Security (Draft for Comments)", which is a relatively high-level administrative regulation and is the same as the "Measures for the Security Assessment of Data Transfer Abroad (Draft for Comments)" which is a departmental regulation. , its nature is to refine and supplement the three-part superior method.

In July 2022, with the promulgation of the "Data Outbound Security Assessment Measures", the scope, conditions, and procedures of data outbound security assessment were specifically implemented, becoming a beacon in the sea of data outbound security assessment. Since then, mainland China's data export legislation has established clear-level and systematic data cross-border governance rules.

It is not difficult to find that the improvement of mainland China's data export legislation is reflected in the higher level of standards, wider coverage, stronger operability, and increased flow permissions, which is in sharp contrast to the early data export legislation.

C. Legal Principles and Reasons for Data Export Supervision

Data is the lifeblood of China's digital transformation and a strategic asset with very important strategic value. Regarding the regulatory legal basis for cross-border data flow, scholar Ding Xiaodong summarizes it into four categories: data without borders, data sovereignty, free trade of data, and cross-border human rights protection of data. This article will follow Ding Xiaodong's classification and further analyze this basis. The legal basis for cross-border travel from Mainland China to the Hong Kong Special Administrative Region.

1. Legal Basis for Cross-Border Data

a. Data Has No Borders and the Legal Principles of Data Sovereignty Do Not Apply

The two concepts of data without borders and data sovereignty do not apply to data export from mainland China to Hong Kong, China. As far as data without borders is concerned, because both mainland China and the Hong Kong Special Administrative Region belong to China, and are essentially data flows within the same country, the legal principle of data without borders does not apply to the situation discussed in this article. In my opinion, the legal theory of data sovereignty is very closely related to the practice of data localization. The concept of data sovereignty means that data should be subject to the laws and regulations of the nation-state where it is generated and processed, which is also a political effort to restrict data services across national borders.[1339] The basis of data sovereignty is the lack of an international legal framework for managing data. In this case, domestic policymakers in each country develop different systems of rules and processes to expand their jurisdictional control over the digital world domestically and internationally.[1340] However, in the context of "one country, two systems" and the Constitution as the fundamental law governing the

[1339] LIU L Z. The Rise of Data Politics: Digital China and the *World. Studies in Comparative International Development*, 2021, 56: 45–67.
[1340] Arner, Douglas W., Castellano, Giuliano G., & Selga, Eriks. The Transnational Data Governance Problem. *Berkeley Technology Law Journal*, 2021, 37(2): 623-699.

"Data Security Law", "Personal Information Protection Law", "Hong Kong Basic Law", etc., it is inappropriate for mainland China and the Hong Kong Special Administrative Region to establish data sovereignty separately. of. At the same time, China is also actively pursuing the "Beijing Effect" and seeking to expand its control and influence over data and data infrastructure globally.[1341] For the above reasons, China has no reason or need to establish two data sovereignty.

b. Data-free Trade and Data Cross-Border Human Rights Protection Cannot Be Transplanted

Free trade in data and cross-border human rights protection mainly reflect the attitudes of the United States and the European Union, and the methods adopted reflect specific cultural, political, economic, and legal characteristics.[1342] Historically, the United States has adopted a laissez-faire approach to data and technology. The complete transferability of data makes the property attribute of data more prominent and obvious. According to the blueprint provided by the "Washington Consensus", the development of the Internet tends to impose minimal regulation on data, creating a frictionless and pro-business environment for cross-border flows.[1343] It is under this model that the United States has given birth to the technology champions of Silicon Valley-Google, Apple, Facebook, Amazon, and Microsoft, becoming the country with the most big tech in the world. However, such a development model is believed by scholar Rogier Creemers to only exist in China before 2020. The emergence of a few large-scale dominant data companies is not what China currently wants to see, because the data outflow of these large-scale dominant data companies is likely to bring security threats in various aspects. The emergency suspension of Didi Chuxing's listing in the United States is very vivid. illustration.

The theory of human rights protection originated in the European Union and has influenced many other countries. Based on this theory, the legal theory of cross-border human rights protection of data has been derived. Underpinned by human rights, Data Governance also aims to embed a rights-based approach to data that reflects Europe's core cultural values and historical experience and to harmonize and extend consumer protection and data privacy across the 27 member states.[1344] However, the EU's approach is closely related to its actual situation. Internally, it established the General Data Protection Regulation and externally set data standards that can confront the United States and influence the world through the Brussels Effect, hoping to maintain its position, taking the line of coordinated market capitalism. The reality of the EU's coordination among its 27 member states is very different from the situation of coordination between mainland China and Hong Kong. China is a major player in digital technology and digital economy. Balancing rights protection and development interests is an urgent need for China. Hong Kong's economic position as a free trade center and constitutional position as a SAR in China give China an upper hand in

---

[1341] MATTHEW S E, THOMAS S. The Beijing Effect: China's 'Digital Silk Road' as Transnational Data Governance, *New York University Journal of International Law And Politics*, 2021, 54(1): 1-92.
[1342] FRANCESCA B, R DANIEL K. Kagan's Atlantic Crossing: Adversarial Legalism, Euro-legalism, and Cooperative Legalism. *GWU Law School Public Law Research Paper*, 2017, 66:1-27.
[1343] Arner, Douglas W., Castellano, Giuliano G., & Selga, Eriks. The Transnational Data Governance Problem. *Berkeley Technology Law Journal*, 2021, 37(2): 623-699.
[1344] ARMIN V B. The European Union as a Human Rights Organization? Human Rights and the Core of the European Union. *Common Market Law Review*, 2000, 37.

developing a more balanced data transfer regime.

c. Legal Basis for Data Governance in Mainland China

Mainland China's regulatory approach to digital competitiveness is characterized by "digital mercantilism" that focuses on ensuring economic stability.[1345] It is a style that revolves around property-based, rights-based, and state-centered data ownership and control. The Chinese data market is characterized by a combination of a property-based approach similar to that in the United States, in the context of private sector acquisition and control of data, and some form of restriction on the introduction of substitution from outside competition, with the government working closely with the non-state sector to reduce risks and achieve broader government objectives. China's regulatory approach is a "unique combination of data protection and government control of data flows", embodying the state-centered approach to ensuring data security.

2. Reasons for Data Export Supervision

Data does not generate or appear alone, and the individuals, companies, and countries behind the data are all separated by national boundaries. The protection of personal rights and interests, property attributes, and national security attached to data need to be regulated. If left unregulated, large multinational corporations will directly dominate the cross-border transmission of data and have power beyond sovereignty. The volume of data exported from mainland companies listed in Hong Kong should not be underestimated. Even if Mainland China and Hong Kong are under the same Chinese sovereignty, data flow from the Mainland to Hong Kong still needs to be regulated.

The first reason is data security considerations. Article 3 of Mainland China's "Data Security Law" stipulates that data security refers to taking necessary measures to ensure that data is in a state of effective protection and legal utilization, as well as the ability to ensure continued security. Article 76, Paragraph 2, of China's Cybersecurity Law, defines "data security" as "the ability to ensure the integrity, confidentiality, and availability of network data." "Confidentiality" here means that the data cannot be obtained by others who should not have access; "integrity" means that the data is not tampered with without authorization or can be quickly discovered after tampering; "availability" means that the data meets the requirements of consistency, accuracy, Timeliness requirements. Even if the data flows from the mainland to Hong Kong rather than abroad, issues of confidentiality and integrity still exist.

The second is out of consideration for protecting personal information. The data export risk management system originated from the protection of personal rights and interests under the cross-border flow of information. Personal information is the most common type of data subject to localized storage requirements, and it is also a category for which mainland China has clarified localized storage of data in its early legislation. Data export may include the transfer of sensitive data such as medical care, health, bank account passwords, genetic information, etc. If not supervised and controlled, personal and property safety information will be leaked, leading to the risk of infringement.

[1345] CYRUS C, PO-CHING L. E-Commerce Mercantilism-Practices and Causes. *Journal Of International Trade Law And Policy*, 2020.

The third is due to national security considerations. In addition to the transfer of sensitive personal data, data export will also include some data containing the economic performance and trends of enterprises and even countries, such as government procurement data, important economic data, involving specific aspects of national politics, society, and economy, and even May contain military data, etc. The importance of these data is self-evident. Due to national security considerations, the aforementioned data should be restricted from exporting abroad, so there is an even greater need to supervise exported data.

The fourth is due to considerations of other legitimate public policy objectives. Since data has property attributes, the data itself can bring economic benefits to the enterprise. If companies are worried about the creative destruction caused by data sharing, companies can hoard data for themselves, but this will limit the positive externalities and welfare benefits that data can generate; Insufficient investment in privacy protection will amplify the negative externalities of data. As noted economist Daron Acemoglu has argued, Big Tech's most pernicious impact stems from their ability to direct technological change, since these companies only have incentives to fund projects that are compatible with their own interests and business models. Research. Therefore, data must not only flow but also circulate on a safe and orderly basis. Risk control of outbound flows is inseparable from outbound supervision.

In summary, it is still necessary and important to supervise the export of data from the mainland to Hong Kong.

D. Data Export: Standards for Data Flow from Mainland China to Hong Kong

The most typical situation where data from mainland China flows to the Hong Kong Special Administrative Region is when companies go public in Hong Kong. As mentioned in the previous introduction, on the one hand, due to the strengthening of cybersecurity supervision of overseas listed companies and the intensification of regulatory friction between China and the United States, there are many obstacles for Chinese companies to list in the United States. The cybersecurity reviews regulatory requirements introduced by mainland China are for those seeking to enter the United States. Chinese companies in the capital market have increased additional transaction costs; on the other hand, the supportive attitude of mainland regulatory agencies towards listing in Hong Kong and Hong Kong's status as a financial center have added confidence and protection to companies listing in Hong Kong. Hong Kong has become China's first choice for corporate IPOs. At present, mainland China has a basic regulatory framework for the rules on the export of personal information, and several departmental laws provide systematic provisions. However, there are still some problems with the lack of specific details and ambiguity of some rules. This part will be elaborated by citing the legal text.

1. Personal Information Export under the "Personal Information Protection Law"

The "Personal Information Protection Law" stipulates five requirements for the transfer of personal information abroad, and specifically formulates rules for the cross-

border provision of personal information in Chapter 3. It is worth pointing out that through the provisions of Article 40 of the "Personal Information Protection Law" plus the exceptions, it can be seen that after reaching a certain level of information importance and information quantity, data export is an exception, that is, in principle, It should be stored within the country and only provided abroad when it is necessary. Only then can information be exported, and many requirements must be met. Article 38 sets out the prerequisites for the export of personal information data abroad, which is the first requirement. This requirement seems to be elaborated in the article by enumerating and adding redundant clauses, which seems to be a relatively comprehensive expression. However, Article 38 (1) mentions "by the provisions of Article 40" The security assessment carried out remains very vague in Article 40. Article 40 of the "Personal Information Protection Law" that came into effect on November 1, 2021, simply outlines the objective conditions of the security assessment. What is the content of the security assessment and what are the criteria for assessment are not specified? However, three days before the "Personal Information Protection Law" came into effect, the Cyberspace Administration of China released the "Data Transfer Security Assessment Measures (Draft for Comments)" to solicit public opinion. In less than a year, the Cyberspace Administration of China issued the "Measures for Data Exit Security Assessment" as departmental regulations. This measure also regulates the subject of data processors as well as the departments, procedures, assessment matters, materials, etc. that apply to data export security assessment. Detailed regulations have been made, stipulating that data processors that process the personal information of more than 1 million people and data processors that have provided personal information of 100,000 people or sensitive personal information of 10,000 people overseas since January 1 last year need to declare. For personal information processors who enter into contracts with overseas recipients by Article 38, paragraph 1, item (3) of the Personal Information Protection Law, there are also "Standard Contract Regulations for the Transfer of Personal Information Abroad" issued in June 2022 (Draft for comments)" can be referred to.

The second and third requirements for the export of personal information are notification and individual consent, which are stipulated in Article 39 of the Personal Information Protection Law. Notification is the special notification obligation of personal information processors in addition to the constraints stipulated in Article 17 of the "Personal Information Protection Law". It is a manifestation of protecting the information subject's right to know, including but not limited to name, contact information, processing purpose, and processing method. etc.; individual consent is "individual consent" in special circumstances, and is a manifestation of the individual's ability to exercise decision-making power.

The fourth and fifth requirements for the export of personal information are personal information protection impact assessment and safeguarding recipient standards. The fourth element is expressly stipulated in Articles 55 and 56 of the Personal Information Protection Law, which adopts an evaluation method similar to the principle of proportionality. The requirement of ensuring recipient standards is stipulated in Article 38, Paragraph 2 of the Personal Information Protection Law, which is also a requirement that this article considers to be very important. When citizens' data flows to jurisdictions that do not provide them with a comparable level of privacy protection, such transfers may undermine privacy objectives, and this concern may further motivate outbound regulators to restrict the free flow of data across borders. The

receiving party's information protection standards largely determine the data exporting party's review attitude toward whether the data can be exported. It is also a solid guarantee for the personal rights and interests behind the data. After all, the first legislative purpose of the "Personal Information Protection Law" The first is "protecting personal information rights and interests", followed by "regulating personal information processing activities" and "promoting the reasonable use of personal information."

To sum up, to protect personal information stored in the Mainland, the state's supervision of personal information data is no different whether it flows from the Mainland to Hong Kong or from the Mainland to abroad. When the amount of information collected and generated by personal information processors in the mainland reaches a certain amount, the regulatory red line of "in principle, the information needs to be stored within the territory" is triggered. If it is really necessary to leave the country, the above five requirements must be met. On the contrary, if it does not reach a certain level, personal information can be provided overseas if any one of the conditions stipulated in Article 38 is met, and the data can be exported abroad.

2. Transfer of Important Information Abroad under the "Cybersecurity Law" and "Data Security Law"

In the "Data Transfer Security Assessment Guide (Draft)", the determination of whether data is important is based on the combination of national security, economic development, and social and public interests, and twenty-eight categories are listed in the appendix. The "Measures for Security Assessment of Data Transfer Abroad" also combines the above three aspects to define important data, but refines social public interests into social stability, public health, and safety. It can be seen that restrictions on the export of important data are largely based on considerations of national security rather than individual rights, and are completely different from the "protection of personal information rights and interests" that is most important in the regulation of the export of personal information.

Article 31 of the "Data Security Law" and Article 37 of the "Cybersecurity Law" both provide for the export of important information abroad. Article 31 of the "Data Security Law" classifies important data according to the holding entities, and stipulates that if important data needs to be provided overseas, a security assessment must be conducted by the methods formulated by the national cybersecurity and informatization department in conjunction with relevant departments of the State Council. It can be seen that even if important information and data flow from the mainland to Hong Kong, data outbound security assessment is an essential link. This article believes that adopting such an attitude is also related to the lack of a framework for data export supervision in the Hong Kong Special Administrative Region. This part will be discussed in Chapter 2 of this article.

It is worth pointing out that Article 13 of the "Network Data Security Management Regulations (Draft for Comments)" considers the data export situation involved in mainland companies listing in Hong Kong separately, and does not review all companies listed in Hong Kong across the board. From the perspective of contextual interpretation, companies listed in Hong Kong that "may affect national security" are

subject to the same cybersecurity review requirements as data processors listed abroad that handle the personal information of more than one million people. Combined with the fourth safety clause, it is not difficult to find that data processors listed in Hong Kong only use "may affect national security" as the premise for declaration because "may affect national security" is the real reason and starting point for supervision. For data processors that do not involve the country, Safe data processors go from the mainland to Hong Kong, which is the so-called overseas listing. The mainland government does not have a strong will to restrict or supervise.

To sum up, when it comes to exporting important data abroad, legislators' main concern is national security. If the data flow from the mainland to Hong Kong does not involve national security and is just a commercial activity, legislators believe that there is no need to interfere too much. However, if the data flow from the mainland to Hong Kong may affect national security, it needs to be subject to the same strict review and supervision as the data flow abroad.

It is worth noting that network security review and data export security assessment may overlap during the operation of the system. For example, if a data-based enterprise has a large amount of personal information in its operations and involves cross-border transmission of data, cross-application will occur. In the absence of a clear applicable relationship between the two in existing regulations, the coordination and connection between the network security review system and the data export security assessment system still need to be further clarified.

II. REGULATION OF MAINLAND DATA RETRIEVAL IN HONG KONG, CHINA

A. Hong Kong's Regulatory Orientation and Development Path for Data Protection

The Hong Kong Special Administrative Region is both an international financial center and the center of massive data inflows and outflows. At the same time, because Hong Kong has a highly transparent regulatory system and a laissez-faire business model, as a major international business center, there are more than 4,000 regional headquarters and offices of leading multinational companies in Hong Kong, attracting a large international data flow.[1346]

Hong Kong's attitude towards data flow has also attracted more cross-border data inflows, forming a positive cycle of "data inflow – free supervision – data inflow – free supervision". This cycle can be specifically reflected in the following: Hong Kong, based on its status as a commercial and financial center, will generate a large amount of inbound and outbound data flows. These cross-border data flows can reduce information asymmetry and improve market access opportunities. They can not only be used for business transactions, supply chain forecasting, market access, and customs processing but can also support cross-border operations necessary for cross-border agreements, ownership of key logistics facilities, and physical and digital delivery of

[1346] Hong Kong Government. LCQ7: Foreign Companies' Regional Headquarters and Offices in Hong Kong. 2021-02-24.https://www.info.gov.hk/gia/general/202102/24/P2021022400302p.htm.

goods and services, bringing benefits and benefits to Hong Kong, and to some extent enhance the city's competitiveness.[1347] Hong Kong, which has enjoyed the dividends brought by data flows, has also been acquiescing to the fact that the law on data export, namely Article 33 of the Personal Data (Privacy) Ordinance (PDPO), has not come into effect. It acquiesces to the prohibition of data localization requirements and is relatively free in supervising data exports. Therefore, Hong Kong's tolerance further attracts the inflow of overseas data.

It can be said that a large amount of data flow is not only the inevitable result of Hong Kong itself as a financial center, but also a means for Hong Kong to further strengthen its position as an international business city and international technology city. As Arner said, the characteristics of each jurisdiction are based on its attitude towards the market and governance, the normative principles that support the exercise of control over data, and the mode of regulating data, and the constantly evolving and unique data governance style.[1348] Hong Kong SAR's current attitude towards cross-border flows is more similar to that of the United States. Compared with the protection of rights and interests, the Hong Kong SAR pays more attention to the commercial benefits brought by the free flow of data.

B. Hong Kong's General Data Protection Model as Reflected in the Personal Data (Privacy) Ordinance

China's Hong Kong Special Administrative Region is the first jurisdiction in Asia to enact comprehensive protection of personal data privacy, and the protection of personal information has always been among the best. As early as 1995, the Hong Kong Special Administrative Region enacted the Personal Data (Privacy) Ordinance. The Office of the Privacy Commissioner has also formulated and issued a series of "New Guidelines on Direct Marketing", "Guidelines on Cross-border Data Transfers", "Guidelines on the Collection and Use of Biometric Data", "Guidelines for Employers and Human Resources Managers" and "Best Practice Guidelines for Mobile Application Development". Guidelines such as "Instructions for Employers to Supervise Employee Work Activities" and "Code of Practice on Identity Card Numbers and Other Identity Codes" help data users understand the relevant provisions of the "Privacy Ordinance" more clearly. In addition, the "Personal Data (Privacy) Ordinance" has been passed many times After comprehensive review and consultation revision, it can be said that the Hong Kong SAR has a relatively complete personal data protection system.

In terms of regulatory entities, the Hong Kong SAR has established the Hong Kong Office of the Privacy Commissioner for Personal Data (PCPD), which monitors and supervises compliance and implementation by issuing guidelines and other measures. The values pursued by the PCPD are respected (respecting the personal data privacy of others), integrity (acting fairly and professionally), innovation (keeping up with technological, social, and economic developments), independence (independence

---

[1347] Hong Kong International Airport.Hong Kong and Shenzhen Airports Sign Cooperation Agreement Join Hands to Promote Airspace Resources Optimisation. 2021-01-04. https://www.hongkongairport.com/en/media-centre/press-release/2016/pr_1200.

[1348] Arner, Douglas W., Castellano, Giuliano G., & Selga, Eriks. The Transnational Data Governance Problem. *Berkeley Technology Law Journal*, 2021, 37(2): 623-699.

from the government and other institutions), and excellence (committed to pursuing Best results and highest standards). This is also mutually confirmed with the legislative purpose of Hong Kong's Personal Data (Privacy) Ordinance, which is "the purpose of the Ordinance is to protect the right to privacy about personal data…". According to the Ordinance, individuals are granted 10 main rights: the right to provide only the required information; the right to collect the information fairly and for lawful purposes; the right to be informed of the purpose of the data; the right to require that the data be accurate; and the right to require that the data not be excessively retained. Rights; the right to refuse consent to change of data use; the right to require data security measures; the right to be informed of data policies and measures; the right to access data; the right to correct data. These ten rights are basic rights related to the protection of personal information, and most of them provide for minimum provision, anytime access and modification, maximum access to purposes, and high convenience for removal.

Combining Hong Kong's Personal Data (Privacy) Ordinance and the value pursuit of the Office of the Privacy Commissioner for Personal Data (PCPD), Hong Kong pays special attention to the protection of privacy when it comes to personal data. The establishment of the Ordinance and the PCPD will protect and respect Personal privacy as the primary pursuit.

C. Hong Kong's Data Re-export Framework

No matter which country or region data is exported to, there is a possibility of secondary export in that country or region, and data exported from mainland China to the Hong Kong SAR is no exception. Therefore, it is necessary to explore Hong Kong's data re-export framework to anticipate possible risks after data is exported abroad.

Hong Kong's "Personal Data (Privacy) Ordinance" takes the protection of personal information and personal privacy as its main legislative tendency and is a conservative protection of personal privacy. According to the provisions of Article 33, paragraph 1, of the Ordinance, the export of data from mainland China After entering the Hong Kong SAR, this batch of data meets the subject requirements of Article 33, paragraph 1, and should also be subject to restrictions on re-exit. Except for the circumstances listed in paragraph 2, it is generally not allowed to re-exit the country. However, the provisions of Article 33 of the Personal Data (Privacy) Ordinance regarding data export abroad have never been implemented, resulting in the Ordinance appearing to be "very generous" in terms of data export.

The debate on whether Article 33 should be implemented in the Hong Kong Special Administrative Region has never ceased, and the minds of legislators are constantly swinging. Hong Kong hopes to participate in the development of global data policies and further promote itself as a sound and stable business place.[1349] In January 2020, the Legislative Council Committee on Constitutional Affairs debated proposed changes to the Personal Data (Privacy) Ordinance. Including mandatory data breach notification mechanisms and data retention periods, and stated that templates and best practice guidelines related to cross-border transfers between institutions and cross-border transfers between cloud processors should be issued; but at the same time, Hong

[1349] Legislative Council Hong Kong.Review of the Personal Data (Privacy) Ordinance. 2020-01-20. https://www. legco.gov.hk/yr19-20/english/panels/ca/papers/ca20200120cb2-512-4-e.pdf.

Kong cannot resist prohibiting data localization on Benefits of own city development competitiveness, prohibiting data localization means allowing data outsourcing, which can reduce the cost of international business and promote openness for multinational companies headquartered in Hong Kong and data-driven enterprises engaged in finance, logistics and innovation and a flexible global technology infrastructure are critical.[1350] Finally, in the amendments to the Personal Data (Privacy) Ordinance published in July 2020, the focus is on combating leaks rather than cross-border data flows. Article 33 on data localization is still pending.

The fact that Article 33 has come into effect does not mean that there are no restrictions on the export of data after it has been transferred to the Hong Kong SAR. The absence of cross-border data restrictions does not mean that users are free to transfer data outside the jurisdiction, as users remain ultimately responsible for their data and are subject to the data protection principles of the Personal Data (Privacy) Ordinance. At the same time, the Office of the Privacy Commissioner for Personal Data in Hong Kong has also issued cross-border data transfer guidelines to help data users understand the requirements after Article 33 comes into effect and provide practical guidance. The PCPD also seeks to encourage data users to adopt the practices recommended in the Guidelines as part of their corporate governance responsibilities.[1351]

It is worth mentioning that Hong Kong's current approach to managing cross-border data flows is consistent with its business approach – it is built on a patchwork of legislation and "default" policies promised by free trade agreements.[1352] Although Hong Kong does not have a clear strategy, policy, or rules to manage data entering and leaving Hong Kong, the Hong Kong government adopts a tacit policy, and individual issues can find guidance in laws and regulations such as the Personal Data (Privacy) Ordinance, and free trade agreements. The commitments made by Hong Kong are also a considerable complement to Hong Kong's efforts in managing cross-border data flows. Hong Kong's commitments in the ASEAN-Hong Kong Free Trade Agreement (AHKFTA Agreement) the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the United States-Mexico-Canada Agreement (USMCA) regarding the free flow of data and prohibition of data localization The promises are similar. By making these commitments, Hong Kong strengthens its ambition to become a global center for receiving, storing, and sharing finance and data, and more broadly demonstrates its goal of maintaining free cross-border data flows.

III. PRACTICAL PROBLEMS IN THE FLOW OF DATA FROM MAINLAND CHINA TO THE HONG KONG SPECIAL ADMINISTRATIVE REGION

[1350] CORY, NIGEL. Cross-Border Data Flows: Where are the Barriers, and What do They Cost?. 2017-05-01. https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost.

[1351] Hong Kong Privacy Commissioner for Personal Data. Guidance on Personal Data Protection in Cross-border Data Transfer. 2017-11-10). https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_ crossborder_e.pdf.

[1352] Mercurio, Bryan. On the Importance of Developing a Coherent Policy Facilitating and Regulating Cross-Border Data Flows. *International Trade Law and Regulation*, 2021(1): 97–104.

A. The Pull between the Development Orientations of the Two Places: Rights or Development?

As mentioned above, due to the needs of data development or the different stages of data development, the legislation and policy trends on data protection and export in mainland China and Hong Kong SAR are not completely consistent, resulting in different data governance styles. Relatively speaking, the Hong Kong Special Administrative Region is more open and mobile and pays more attention to regional development in rights protection and regional development, while Mainland China attaches more importance to localized storage and strives to find stable development and stable protection in rights protection and regional development. balance.

Before 2009, the Chinese government largely followed U.S. practices regarding private data within China, but over the past decade, the Chinese government has tightened controls on the flow of data in and out of China, controlling access to data at home and abroad, Monitoring, regulating and controlling the monopoly power created by the concentration of data sent or collected by large technology companies, eventually almost eliminating large IT companies such as Google, Apple, Meta, Amazon, Microsoft (GAFAM) from the domestic market, hoping to cultivate A competitive local leading enterprise. In the process of controlling the expansion of large IT companies, the Chinese government will inevitably have some impact on the Hong Kong Special Administrative Region, which aspires to economic development. However, data shows that mainland China's target of large technology companies has temporarily affected the stock prices of these companies on local exchanges. It only affected Hong Kong indirectly, but many experts are still worried that the impact may be more direct in the future.

Although mainland China's legislative provisions only apply to all companies operating in China, laws and regulations such as the "Personal Information Protection Law" and "Data Export Security Assessment Measures" cannot be applied to the Hong Kong SAR, these provisions may still have an impact on Hong Kong. The special zone has a significant impact. Among the new rules introduced by Beijing in the past five years, companies are required to obtain government approval before transferring certain types of data outside China, as part of a broader government effort to tighten controls over data and protect national security. Hong Kong has long been a hub for international companies to enter the mainland market. Many multinational companies have established regional headquarters in Hong Kong, hoping to ride on Hong Kong's proximity to mainland China and its status as a global financial center. The promulgation of these new regulations may prevent these multinational companies from storing sensitive data in Hong Kong, making it more difficult for these multinational companies to operate in Hong Kong, China.

This is evident from the pull between the development orientations of the two places. Hong Kong's economy is highly dependent on its role as the world's gateway to mainland China. According to a report by the Hong Kong Trade Development Council, about 60% of Hong Kong's exports are re-exports - goods imported into Hong Kong from countries around the world, which are then re-exported to other markets, including goods entering mainland China. If foreign companies are forced to store data on the mainland, this could undermine Hong Kong's status as a center for import and export

transactions, as it will not be able to offer the same level of data privacy and security as other global financial centers. Hong Kong's status as a global financial center may also be affected. If multinational banks and financial institutions that set up operations in Hong Kong realize that Hong Kong can no longer provide them with a good business environment and the costs of operations and compliance have greatly increased, they are likely to Move to other financial centers in Asia, such as Singapore.

In general, the promulgation of new regulations on the mainland in the past five years has posed new challenges to Hong Kong's development. However, this article believes that new challenges do not mean that they will bring new disadvantages to the Hong Kong region, or hinder the development of the Hong Kong region. The mainland and Hong Kong are each part of China. Although the systems are different, they should both make efforts for data control and maintain National Security. However, how to achieve common development still requires the mainland and Hong Kong to think and work together.

B. Tightening of Legal Regulations Between the Two Places: Hong Kong Has Become a Shortcoming in Data Export

Since the laws and regulations of mainland China and the laws and regulations of Hong Kong are at different times, have different levels of development, and have different tightness of regulations, whether the two places are fully aligned in terms of data export and whether there is an overlap or vacuum in supervision is something that this article believes needs to be discussed. The author compared Hong Kong's Personal Data (Privacy) Ordinance and Mainland China's Personal Information Protection Law in terms of legislative purposes, the definition of "personal data", consent models, fines, corporate compliance qualifications, and codes of conduct. In terms of legislative purposes, it is not difficult to find that Hong Kong's regulations do not clearly state "promoting the reasonable use of personal information", but it is mentioned in the Mainland's "Personal Information Protection Law". This does not mean that personal information in Hong Kong currently adopts a conservative approach to rights protection, but because Hong Kong's Personal Data (Privacy) Ordinance has been enacted for a long time and has not been revised and updated promptly for legislative purposes. This also reflects that because Hong Kong enacted regulations earlier, with the development of the times and technology, there is some lag, which may create loopholes in the protection of personal data.

In terms of the definition of personal data, Hong Kong stipulates that the subject of personal data must be a living individual, while the Mainland's "Personal Information Protection Law" stipulates that the subject of personal information only requires natural persons, and does not require the natural person to be alive. The first problem that may arise from this is that during the process of data export, if the personal information of a deceased person is transmitted, the protection that can be obtained in the mainland is not available in the Hong Kong SAR, resulting in data protection. on the fault. In addition, Hong Kong does not specifically distinguish between personal information and personal sensitive information, while the mainland classifies personal data in regulations such as the "Guidelines for Security Assessment of Information Security Technology Data Transfer (Draft)" and stipulates personal information and personal sensitive information. Different types of information are given different levels of protection, which will lead to the problem that data from mainland China can no longer

receive the same level of protection after being exported abroad.

In terms of penalties, according to Hong Kong laws and regulations, violations of the regulations can be punished with a maximum penalty of HK$1 million (approximately 880,000 yuan) and five years of imprisonment. According to mainland regulations, a maximum penalty of not more than 50 million yuan or a turnover of 100 million yuan in the previous year can also be imposed. A fine of not more than five-fifths of the amount shall be imposed, and a fine of not less than RMB 100,000 but not more than RMB 1,000,000 shall be imposed on the directly responsible person in charge and other directly responsible personnel. Judging from the intensity of fines, the penalties in the Mainland are even higher, especially for enterprises, especially large enterprises. The turnover of less than 5% of the previous year is likely to be much higher than the one million Hong Kong dollar cap stipulated in Hong Kong. In terms of the objects of punishment, Hong Kong's current laws only stipulate personal liability, while mainland laws distinguish between individual liability and corporate liability. Enterprises not only face high financial penalties, but also may be ordered to suspend relevant business or suspend business for rectification or notify Relevant competent authorities will revoke relevant business licenses or revoke business licenses, and be subject to administrative penalties. Today's enterprises are increasingly adopting data-driven business models and strategies to gain and sustain a competitive "data advantage" over their opponents. Generally speaking, a reduction in the cost of violating the law is likely to lead to an increase in violations. Under the economic thinking model of cost-benefit analysis, when the cost of violating the law is too low and is lower than the benefits obtained from data flow, companies as data controllers are likely to take risks and would rather pay fines than use Hong Kong to complete data entry and exit.

Generally speaking, the degree of tightness of legal regulations in the two places is different. Hong Kong's relatively free and relaxed regulations make Hong Kong likely to become a shortcoming in data export, overriding the protection of data under mainland China's laws and regulations, and causing many practical problems.

IV. POSSIBLE LEGAL SOLUTIONS FOR DATA FLOW FROM MAINLAND CHINA TO THE HONG KONG SAR

Huang Ning and Li Yang pointed out that there are three difficulties in the regulation of cross-border data flows, that is, "good data protection", "free flow of cross-border data" and "data protection autonomy" of various governments cannot be achieved at the same time[1353]; D. W. Arner pointed out that the domestic governance styles of each country are consolidated into competing and conflicting data governance systems, the transnational output and influence of various countries are destroying the existing transnational data governance paradigm based on the free flow of data and hindering international coordination in the global data economy. [1354] This is transnational data. the wicked problem of transnational data governance because there

[1353] 黄宁,李杨."三难选择"下跨境数据流动规制的演进与成因.清华大学学报(哲学社会科学版),2017,32(05):172-182+199.

[1354] Arner, Douglas W., Castellano, Giuliano G., & Selga, Eriks. The Transnational Data Governance Problem. *Berkeley Technology Law Journal*, 2021, 37(2): 623-699.

is no single solution to it.[1355] It can be said that data export cannot take into account both the protection and flow needs of data at the transnational level. The balance will inevitably be more or less tilted towards a certain value. However, this article believes that it contains the possible laws of data flow from mainland China to the Hong Kong Special Administrative Region. solution. The reason why data governance mechanisms are different is due to conflicts of national interests. However, it can be seen that there is no conflict of national interests between mainland China and Hong Kong, and it is entirely possible to achieve win-win results.

A. Jointly Negotiate to Establish Data Circulation and Transaction Standards Suitable for the Characteristics of Greater China

Various laws and regulations promulgated by mainland China in the past five years have indirectly affected Hong Kong, and at the same time, they have also brought new opportunities and challenges to Hong Kong. Under the basic framework of one country, and two systems, the mainland and Hong Kong can jointly negotiate and establish data circulation and transaction standards that suit the characteristics of Greater China.

Allowing some freedom for cross-border data flows would benefit both Hong Kong and the mainland. With more than 700 million internet users across China, leading technology manufacturing companies such as Huawei and Lenovo, and growing technology giants such as Alibaba, Baidu, and Tencent, allowing partial freedom in the flow of data across borders would not only allow Hong Kong to maintain its position among multinational companies The competitiveness in mind will also bring obvious economic benefits to the mainland due to the cross-border flow of data. In addition, China's local technology companies also have plans and ambitions to enter the global market. If too many restrictions are imposed on cross-border data flows, it may hinder the development of these companies' global operations and reduce their competitiveness. At the same time, controlled freedom in cross-border data flows can also prompt Hong Kong to strengthen its legal framework for data protection and privacy. This will not only attract companies and maintain its status as a global financial center but also help Hong Kong in building "Asia's largest financial center". One of the "Secure Data Center Cities".

Hong Kong and the Mainland should jointly negotiate to establish data circulation and transaction standards suitable for the characteristics of Greater China, and discuss how to strike an appropriate balance in supervision while providing appropriate deterrence without compromising the interests of innovation, collaboration, and improving business efficiency. In the "14th Five-Year Plan" announced in March 2021, the mainland has established the goal of developing an innovative country and a technological power, and proposed a development pattern of "domestic large cycle and domestic and international dual cycle" to develop the Guangdong-Hong Kong-Macao Greater Bay Area. Become an international science and technology innovation center. Hong Kong also stated in the "Hong Kong Innovation and Technology Development Blueprint" that Goal 01 is to promote the effective flow of innovation elements across borders, strengthen the competitiveness of Hong Kong's innovation and technology,

---

[1355] Pedch U, E., Vermass P. The Wickedness of Rittel and Webber's Dilemmas. *Administration and Society*, 2020,52:960.

and better serve the needs of the country. Measures to achieve the goal include exploring with mainland ministries and commissions Implement more measures to promote the convenient cross-border flow of innovative elements. In terms of data, we will actively study with the mainland on specific facilitation arrangements to promote the flow of data from the mainland to Hong Kong and launch a pilot plan for cross-border data flow in the Greater Bay Area in 2023 to test Technical standards, measures and data governance mechanisms for widespread implementation in the future. Both sides have shown an attitude of active consultation, cooperation, and putting national interests first. If a data exchange agreement mechanism between mainland China and Hong Kong, or even Hong Kong, Macao, and Taiwan can be established shortly, it will be of great benefit to the development of both places.

B. Hong Kong Promotes Article 33 of the Ordinance to Take Effect as Soon as Possible to Fill the Shortcomings of Data Export Regime

Hong Kong hopes to consolidate its advantages as a data center in the Asia-Pacific region, not by becoming an "outbound paradise", but by promoting Article 33 of the Ordinance to take effect as soon as possible. Mainland China's laws have tended to regulate data exported to the Hong Kong Special Administrative Region and exported to foreign countries separately, because China is well aware that Hong Kong is still a part of China, and there is no national-level political and economic conflict between the mainland and Hong Kong. It can be said that All data is transferred between people. At present, the "Regulations (Draft for Comments)" have set different application conditions for data processors listed abroad and listed in Hong Kong, China. It is foreseeable that after the mainland laws and regulations are improved, the export of data to Hong Kong should be more relaxed than the export of data. To design abroad. To comprehensively regulate and manage privacy, Hong Kong should implement or amend Article 33 of the Ordinance to fill the shortcomings of data export so that Article 33 will no longer become a "backdoor shortcut" for multinational companies to enter the Chinese market.

C. Legal and Administrative Integration Between Hong Kong and the Mainland

It is recommended that Hong Kong and the Mainland align themselves on the administrative management of data export abroad. The author believes that although the EU is an attempt to establish a single market between countries and is somewhat different from China's national conditions of one country, two systems, some of the EU's practices are worth learning from. To manage data in a single unit, the EU launched the European Cloud initiative to simplify data access by seamlessly moving, sharing, and reusing data across European markets and borders. The EU is also creating its own data walled garden, designed to connect cloud providers across Europe, harmonize technology standards, and ensure data privacy and security walls. The author believes that we might as well set up a supervisory and management agency for data transmission from mainland China to the Hong Kong SAR. Currently, the cross-border data flow between the Mainland and the Hong Kong SAR is managed separately by different agencies on both sides. This will, to some extent, lead to the lack of an effective unified management mechanism and hinder cross-border data flow.

It is recommended that Hong Kong and the Mainland align with the legal

regulations on data export abroad. The Organization for Economic Co-operation and Development (OECD) advocates a more detailed differentiation of personal data based on international standards and divides technologies into five categories of data identification: (1) identifying data, (2) pseudonymous data, (3) unlinked pseudonyms Data, (4) Anonymous Data and (5) Aggregated Data. At present, mainland laws distinguish personal data, but it is not as detailed as advocated by the Organization for Economic Cooperation and Development. It may be further refined in the future. However, Hong Kong law has not yet distinguished personal data, and it needs to be revised and improved. The current development of data analytics and artificial intelligence has made it easier to link seemingly non-personal data with identified or identifiable individuals. The concept of "personal data" is constantly changing and is no longer as stable as it was when the Ordinance was originally formulated. definition, Hong Kong should take advantage of the opportunity to update the existing structure. Because a higher level of protection of personal data rights will also enhance consumer confidence in digital trade and stimulate economic development, the mainland and Hong Kong may wish to align on the legal regulations on data export, learn from each other's strengths, and eliminate the shortcomings of national security loopholes in data. plate. Before the legal integration, if a certain number of companies can achieve a high level of privacy protection, they can also learn from the "safe harbor" model and have the governments of the two places negotiate and sign bilateral data flow agreements.

D. Special Legal Arrangement for Data Transfer within the Guangdong-Hong Kong-Macao Greater Bay Area (GBA)

In December 2023, the Cybersecurity Administration of China (CAC), China's top cybersecurity authority, released a new set of guidelines for companies in the Guangdong-Hong Kong-Macao Greater Bay Area (GBA) to sign a standard contract to engage in cross-border personal information (PI) transfer between the mainland portion of the GBA and Hong Kong. The GBA (Mainland, Hong Kong) Implementation Guidelines for the Standard Contract for Cross-border Flow of Personal Information (the "GBA guidelines") are the result of an agreement between the CAC and the Innovation, Technology, and Industry Bureau (ITIB) of Hong Kong to facilitate cross-border data flows and establish security rules for PI transfer within the GBA. The GBA guidelines, which took effect on December 13, 2023, make it significantly easier for companies located in one of the nine mainland cities of the GBA to transfer personal information to Hong Kong by expanding the scope of companies permitted to use the standard contract procedure, as well as simplifying filing procedures. The efforts to streamline cross-border PI transfer align with the central goal of deepening integration between the mainland and offshore areas of the GBA and fostering a more business-friendly environment in the region. This is a positive development towards a sound legal framework for data transfer between the Mainland and Hong Kong.

CONCLUSION

The constitutional basis for the establishment of the Hong Kong Special Administrative Region is Article 31 of the Constitution. As the fundamental law, Article 31 of the Constitution constitutes the legal basis of "one country". Since Hong Kong returned to the motherland in 1997, it has enjoyed a "high degree of autonomy" under the authorization of the central government. The opportunities brought by "two systems" have made Hong Kong an important link between the mainland market and

the international market. Under the Constitution, the relationship between the mainland and Hong Kong follows the principle of "one country, two systems". Within the framework of one China, the mainland and Hong Kong maintain their respective systems and development models. Therefore, although data flows from the mainland to Hong Kong, China, it is data outbound, but the data has never left the country. The transmission of data from the mainland to Hong Kong essentially still belongs to the free flow of data within a country. Problems that may arise during the flow of data can be solved through the improvement of internal laws, the connection of internal administration, and the standardization of internal systems.

In an era when the value-generating function of data is growing, we should make good use of the convenience and advantages of "one country" and "two systems", seize opportunities, use the value of data to achieve national development and protect the rights of the people while developing. There is reason to believe that with the continuous improvement and integration of laws, the continued in-depth cooperation between the two places, and the continuous advancement of technology, the cross-border data flow from mainland China to the Hong Kong SAR will be safer, more reliable and more convenient in the future. China The mainland and Hong Kong as a whole will stand on the international stage and make greater contributions to the development of the global digitalization process.