Research on Data Sovereignty Rules in Cross-border Data Flow  
and Chinese Solution

CHEN Si  
University of International Business and Economics, Beijing, China

Data sovereignty is the manifestation of national sovereignty in the digital field, which is also a matter of national security. While the U.S. ostensibly emphasizes the cross-border free flow of data, it actually implements the powerful policy of long-arm jurisdiction damaging the data sovereignty of other countries. On the other hand, the EU promotes European rules to the world in the name of advocating data protection, furthering data sovereignty through technological sovereignty. Russia asserts data sovereignty by adopting data localization measures. In order to adequately maintain data sovereignty in the cross-border flow of data as well, China should draw up the extraterritorial practice of relevant rules. In view of the problems to Chinese data sovereignty rules, we propose the concept of constructing such to strike a balance between data protection and data open, establish the jurisdictional rules of data sovereignty, determine the reasonable scope of applying data localization, and actively participate in the international legislation of data sovereignty. The proposal is also to provide a Chinese solution that is prudent and encouraging cooperation for global data sovereignty rules.

Keywords: data sovereignty, cross-border data flow, data localization

Introduction

Data sovereignty is the expression of national sovereignty in the field of data. While facilitating the development of digital economy and digital globalization processes, the cross-border flow of data can also pose a threat to national security and sovereignty, namely endangering the data sovereignty of one country. In order to maximize national data sovereignty, countries have already developed certain rules to regulate the cross-border flow of data. For example, the United States also imposed sanctions on TikTok\(^1\) in August 2020 on the grounds of maintaining data sovereignty, prohibiting TikTok’s data traffic in the United States and requiring TikTok to sell all of its operations in the United States to prevent it from collecting or using U.S. data. Moreover, in July 2021, the United States Securities and Exchange Commission (SEC) required Didi, a Chinese company listed in the United States stock market, to disclose its operational data. The operational data involves information of Chinese roads, Didi vehicles and users, which, if leaked, is likely to violate the personal privacy of Chinese citizens and even endanger our national security and data sovereignty. In order to prevent the United States from accessing sensitive Chinese data, China had also conducted a cyber security review of Didi, before urgently

\(^{1}\) TikTok is a short video platform launched in the U.S. in May 2017 under Byte Dance.
taking down the “Didi Chu Xing App” from the app stores. In August 2021, Luxembourg, as an EU member state, imposed a fine of €746 million on U.S.-based Amazon.com for use of users’ personal data without their consent, also reflecting the defense of their data sovereignty. This series of events reflects the determination of various countries to maintain data sovereignty in cross-border data flows.

As a country with large amounts of cross-border data flow, how to maintain data sovereignty is also one of the national security challenges that China is facing. This paper compares and analyzes the relevant regulations on data sovereignty in the United States, Europe, and Russia as well as international Free Trade Agreements on cross-border data flows influential to China, appraises the current situation and problems of data sovereignty rules in China, and puts forward suggestions for constructing data sovereignty rules of Chinese characteristics.

The Extraterritorial Practice of Data Sovereignty Rules

U.S. Data Sovereignty Rules

The U.S. has an extremely dominant position in the field of cross-border data flow, and in order to maintain national data sovereignty, achieving the America First policy and the goal of long-arm jurisdiction, the U.S. actively adopts the intra-territorial jurisdiction model based on the principle of personal jurisdiction and the extraterritorial jurisdiction model supplemented by the principle of minimum connection.

In the Microsoft Corp. v. United States case, Microsoft refused to provide the U.S. government with data related to the suspect’s account and stored on an offshore server, on the grounds that the U.S. government did not have jurisdiction over data stored abroad.2 The case suggested to the U.S. about the data sovereignty risks that can arise in the cross-border flow of data, and in March 2018, the U.S. passed the Clarifying Overseas Use of Data Act (the “Cloud Act”), which redefined the boundaries of U.S. data sovereignty.3

In terms of internal jurisdiction, the U.S. adopted the Cloud Act to confirm for the first time that the authority of government agencies to access data in the possession, custody or control of companies is not limited by the location of data storage. Following the principle of personal jurisdiction, any data involving U.S. citizens, whether stored within or outside the country, need to be strictly under the jurisdiction of U.S. law and protected by the right to privacy, while no other country can unilaterally access the data. In terms of external jurisdiction, the U.S. ostensibly promotes the free flow of data across borders, but, in essence, consolidates its established data dominance by imposing long-arm jurisdiction over data globally. The U.S. has expanded the scope of its data sovereignty through the Cloud Act, which provides a legal basis to exercise and expand long-arm jurisdiction through the minimum contacts doctrine.4 The U.S. has adopted the principles of personal jurisdiction and minimum connection to maintain its data sovereignty and protect national data security, while also focusing on the collection and utilization of global data resources, as well as forming a “lenient entry and strict exit” model.

---

2 See United States v. Microsoft Corp., 829 F. 3d 197 (2d Cir. 2016), at 217-218.
3 In re Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y. 2014), United States District Court, S. D. New York, April 25, 2014, at 467.
4 Originally used as the basis for the court’s determination of jurisdiction in International Shoe Co. v. Washington State, the doctrine of minimum contacts means that the United States has jurisdiction over any business or person internationally, so long as their conduct has a connection to the United States.
First, the U.S. continues to promote a data sovereignty strategy in the international community that allows data to flow into the country, strongly advocating the benefits of free cross-border flow of data. Relying on its absolute advantage in this field, it dominates other countries in setting the rules of data sovereignty. Since 2017, a series of cross-border cooperation agreements, including the Korea-U.S. Free Trade Agreement, the Trans-Pacific Partnership Agreement, the Transatlantic Trade and Investment Partnership Agreement, the U.S.-Mexico-Canada Agreement, and the Asia-Pacific Economic Cooperation (APEC) with “Cross-Border Privacy Rule” regime, have been reached, all of which promote free and easy cross-border flow of data from other countries into the United States.

Second, the United States severely restricts access to U.S. data by foreign governments or companies unless it has already entered into an administrative data sharing agreement with a U.S. government agency. The agreement may only be effective after the foreign government or company certifies in writing to the U.S. Attorney General and Secretary of State that strong substantive and procedural safeguards for personal data privacy have been provided, and the foreign government or company must also agree to share the relevant data it holds with U.S. government agencies. In addition, U.S. government agencies will review and update this administrative data sharing agreement every five years to ensure that the above requirements are fully met. As you can see, only eligible foreign governments or companies can access data within the United States, and the access process is complex and cumbersome. The Cloud Act ostensibly enriches the channels and modes of government-to-government access to transnational data, but in essence further strengthens U.S. control of data. The U.S. combines the advantages of both its digital platform operators and equipment providers in the international marketplace, to strengthen U.S. control and extraterritorial jurisdiction over its own data, while ensuring strong U.S. control over data in cross-border flows and safeguarding the U.S. data sovereignty advantage (Huang & He, 2019). In 2019, the U.S. enacted the National Security and Personal Data Protection Act, which gives more prominence to the assertion of data sovereignty. The Act explicitly prohibits any U.S. company from transferring any data it collects within the U.S. and outside the country, while forbidding any foreign country or business from collecting and storing U.S. data.

Finally, the U.S. has strengthened its management of critical data infrastructure. For example, China is designated by the U.S. as a country of special concern and is under data security assessments on a yearly basis, while several Chinese high-tech companies are included in the list of entities subject to sanctions and domestic U.S. companies are strictly prohibited from doing business with them.

**EU Data Sovereignty Rules**

The tight control of data by the United States puts Europe as a whole at an extreme disadvantage in asserting data sovereignty, and the EU must actively seek effective ways to respond. The General Data Protection Regulation (GDPR) by the EU, which came into effect in 2018, provided a unified Pan-European Legal Framework for cross-border data flow, removed barriers to cross-border data flow between EU countries, and began to gradually penetrate the world with the influence of European rules related to data sovereignty.

First, the GDPR establishes data protection rules to safeguard data sovereignty and expands the scope of data sovereignty jurisdiction. The GDPR provides for the development of a data protection authority at the

---

5 18 U.S.C.A. § 2523(b)(1) (2018).
location of the primary institution of the data controller or processor to protect and control data, as well as establishes compensation and penalty mechanisms for violations of data protection rules.\textsuperscript{6} For example, in March 2021, the Spanish Data Protection Agency fined Vodafone a total of €8.15 million for improperly processing personal data during its marketing campaigns from 2018 to 2020, in violation of EU data protection rules (Ding, 2018). In addition, the GDPR clarifies the EU adoption of data control standards, i.e., regardless of whether the data is stored in the EU geographically, as long as it is stored on a data server controlled by an EU data service provider, the EU is considered to receive control and processing rights over that data. It can be seen that the EU has adopted a means similar to the U.S. long-arm jurisdiction to expand the scope of exercising its data sovereignty.

Secondly, to demonstrate its data protection concept, the EU proposes to confirm whether other countries can adequately protect data security through “adequacy determination” and “appropriateness guarantee”. An “adequacy determination” means that the EU prohibits the transfer of data to countries outside the EU unless the recipient country can demonstrate an equivalent level of data protection to EU standards. Only countries that have met the EU determination criteria, have received an EU adequacy decision, and have been included in the “white list” are eligible to exchange data across borders with EU countries. Nations that are not on the “white list” are required to provide “adequacy safeguards” to be allowed on cross-border data flows. This ensures that data sovereignty is not infringed within the EU and undoubtedly strengthens the impact of European data sovereignty rules on the global regulatory landscape for cross-border data flows (Ye, 2020, p. 110).

Finally, the inherent logic of the EU’s assertion of data sovereignty is to expand it through technological sovereignty from enhancing technological power. In 2019, the president of the European Commission proposed the concept of “technological sovereignty” (Zhou, 2020), emphasizing that Europe should use technological sovereignty to establish and vigorously implement its own data sovereignty rules in order to gain control in the digital economy. The EU continued to make a push in 2020 over the area of data sovereignty, proposing new rules for European data sovereignty through new technologies, such as big data and artificial intelligence of critical infrastructure and data security (Jiang, 2021). In July 2020, the EU released the report “Digital Sovereignty in Europe”, with aims to place the EU focus on technological sovereignty to introduce its data governance and data sovereignty rules to the world, as well as reduce dependence on other countries for data-critical technologies, and counter the appropriation of data by foreign data servers. The EU has also created a “European cloud” system called Gaia-X to provide a secure and unified infrastructure framework of data storage to facilitate data flows and data protection among EU member states (Jiménez-Gómez, 2021).

**Russian Data Sovereignty Rules**

Unlike the United States and the European Union, Russia has always taken a conservative approach to cross-border data flows due to its own disadvantages in data market, adhering to a single territorial jurisdiction principle, i.e., a data localization model to strictly control data flows in the country.

First of all, Russia, based on data security consideration, always puts data sovereignty at the forefront of national security through the data localization model, and strictly enforces the priority of data localization to ensure domestic data security. In 2006, Russia enacted the Federal Law on Personal Data, which established a

\textsuperscript{6} See the Guidelines on the Lead Supervisory Authority WP244 rev.01 of 31 October 2017 (EDPB).
very strict data protection regime that required companies to use and store data only within Russia (Orlova, 2020). In 2014, Russia amended the Federal Law on Personal Data to require data service operators to use data storage systems only within the country, and, in July 2017, Russia enacted the Law on Critical Data Infrastructure, which prohibited the use of software and hardware to access Internet resources that have been blocked by Russia. In 2019, Russia enacted the Sovereign Internet Law, which established autonomous and controlled data sovereignty in the traditional infrastructure of critical information and introduced a new rule of “active disconnection” of data (Wang & Liu, 2020). The rule provides that the Russian Federal Service for Supervision of Telecommunications, Information Technologies and Mass Media has the right to actively disconnect the domestic network from the external Internet in the event of an external data intrusion that threatens the network, with the aim to defend the Russian network stability. Russia has effectively circumvented extraterritorial interference of data control from the U.S. and EU through a strict data localization model, and has maintained its data sovereignty.

Second, Russia has strengthened its data infrastructure to reinforce its ability to withstand external data risks. Since the Prism in 2013, Russia has proposed to improve the data security system of the national computing facilities and to enhance the monitoring and protection of data security (Zhang, Cai, & Zhang, 2017). Russia has successively required enterprises to prioritize the use of state-owned technological equipment, increase the proportion of Chinese-developed products in the data infrastructure, develop a protective early warning system for computing facilities, and safeguard national data sovereignty by strengthening the data infrastructure. In 2019, Russia proposed a national cyber strategy to further optimize the hardware equipment of critical data infrastructure, to avoid being subjected to foreign countries in critical computing equipment, and to strengthen the ability to resist external data risks.

It is thus clear that Russia places more emphasis on the political interests of the country and the need to maintain the country’s political stability than on the economic interests. The adoption of the data localization model based on the principle of single territorial jurisdiction reflects Russia’s strong sense of preserving data sovereignty rather than the economic benefits brought by the cross-border flow of data.

**Data Rules for Our Participation in Free Trade Agreements**

At present, the international rules directly related to China’s cross-border data flow are mainly the Trans-Pacific Partnership Agreement (CPTPP), Digital Economy Partnership Agreement (DEPA), and Regional Comprehensive Economic Partnership (RCEP). Whether it is the CPTPP and DEPA that China is applying to join, or the RCEP that China is participating in, the principle of data sovereignty is still upheld for cross-border data flow. Article 14.13 of the CPTPP provides that any member country shall not grant the conduct of its business within its territory on condition of the use or establishment of computing facilities within its territory. It can be seen that the CPTPP sets up an exception clause for cross-border flow of data, holding that each member country should actively carry out cross-border flow of data on the basis of infringing on no data sovereignty and safeguarding common interest by prohibiting the localization of computing facilities. 

DEPA allows the free flow of data cross-border of agreement members in the data issue module, and sets non-mandatory locational restrictions on computing devices to provide maximum inclusiveness for data sovereignty of member countries and to promote data sovereignty cooperative jurisdiction among member
countries. The modular innovation of DEPA integrates data sovereignty and data economy development, and also
provides new ideas for international rules on data sovereignty.

The signing of RECP marks China’s participation in the largest free trade agreement in the world and this is
the highest level of international rules for China’s participation in the data field at this stage. RCEP explicitly
prohibits data localization and encourages the free cross-border flow of data. National security exceptions are
added to the CPTPP clauses, to which other member countries are not allowed to object. This reflects the RCEP’s
recognition and the maintenance of national sovereignty.

A notable trend in the data field is that sovereign countries have been asserting data sovereignty by means of
improved legislation. Whether it is to deal with the impact caused by cross-border data flow or to adapt for the
requirements of data sovereignty rules in regional free trade agreements led by CPTPP, DEPA, and RCEP, there
is an urgent need for China to build its own data sovereignty rules to maintain national security.

The Current Situation and Problems of Data Sovereignty Rules in China

Status of Data Sovereignty Rules in China

Before the formal implementation of the Cyber Security Law, the form of data governance in China was
mainly manifested as independent regulation by industry. For example, the “Notice of the People’s Bank of
China on the Proper Protection of Personal Financial Information by Banking Financial Institutions” provides for
the governance of personal financial data, including the collection and use of it by financial institutions. “The
Population Health Information Management Approach” (for Trial Implementation) addresses population health
data, such as electronic health records and electronic medical records, and proposes to strengthen the
management and security of these data. “The Interim Measures for the Management of Network Reservation
Rental Car Operation Services” implements various data protection measures for platforms and regulations
related to the data security of car renters. Although sub-sector independent regulation can protect personal data
generated in key areas such as people’s livelihood and economy to a certain extent, it cannot cope with the brand
new challenges to national security brought by the cross-border flow of data. At this time, China’s legal
framework for cyber security has not yet been established, lacking systematic regulation of cross-border data
flows, and short of measures to uphold the rules of data sovereignty, which can only be maintained to a certain
extent through data localization.

In 2017, the Cyber Security Law was formally implemented, building a systematic legal system for cyber
security and imposing regulatory requirements on the cross-border flow of data. The concept of data sovereignty
is spawned by the spillover effect of state control in the process of cross-border data flow, where the
jurisdiction of state sovereignty is no longer clear-cut, resulting in the infringement of countries’ right to data
independence and control. Data sovereignty is the state’s right to manage and control data with its related
technology and equipment, which is essentially a direct application of the Westphalian concept of sovereignty to
the data domain. Under the Westphalian system, data sovereignty is expressed as an extension of state
sovereignty in the field of data, which is reflected internally in the state’s supreme jurisdiction over data as well as
externally in the state’s independent autonomy and cooperation over data (Sun & Zhang, 2015). In order to
strengthen the control of data, the Cyber Security Law mainly adopts the principle of territorial jurisdiction. By
introducing the concept of “critical information infrastructure”, emphasizing the construction of critical
data sovereignty, which is a milestone in the construction of data sovereignty rules.

On June 10, 2021, China adopted the Data Security Law, which establishes an infrastructure for data security in China, puts forward the “Data Security in Free Flow Principle” for the first time, and proposes to establish a data classification and protection system, actively carries out data security reviews, and intensifies the crackdown on data flows that threaten national security, with the aim of safeguarding data sovereignty by ensuring data security (Xu, 2021). At the same time, this law advocates the improvement of data security assessment in China.

On October 29, 2021, the State Internet Information Office published the “Measures on Data Exit Security Assessment (Draft for Comments)”. Since outbound data may trigger national security and data sovereignty risks, this draft for public opinion put forward assessment requirements for China’s outbound data, and stipulated that safeguarding outbound data security is also a manifestation of safeguarding data sovereignty.

**Problems of Existing Data Sovereignty Rules in China**

The formulation of data sovereignty rules in China started late and the legal system regulating data is not yet perfect. After the promulgation of the Cyber Security Law, the Data Security Law and the Personal Information Protection Law, the legal framework for data protection in China is basically established, but the following problems still exist.

**Legislative level: Lack of extremely binding and influential data legislation.** Due to the late start of data sovereignty governance in China and the limited time for data sovereignty system construction, we cannot establish a systematic and internationally influential data sovereignty governance system, like the United States and the European Union, and we cannot participate well in the formulation of international rules on data sovereignty. This is not conducive to realizing the systematic governance of national data security and data sovereignty, or to realizing the economic benefits of data in the era of digital economy globalization. At present, China’s data sovereignty legislation mainly revolves around the Network Security Law and the Data Security Law, although China has continuously made additions in the areas of data exit security assessment and data technology security, a legal system with strong binding and influential data sovereignty regulation has not yet been optimized.

**Protection measures level: Advocating overly strict measures of data localization.** Currently, developed countries tend to adopt a lenient strategy towards cross-border data flows in order to maintain their first-mover advantage over data domain. For example, the U.S. maintains a very open attitude toward cross-border data flows, and the EU is influenced by the U.S. data sovereignty rules to take a both offensive and defensive attitude toward cross-border data flows. Developing countries and underdeveloped countries mainly adopt data defense measures to maintain national data sovereignty, and China also adopts a conservative attitude. Article 37 of the Cyber Security Law still advocates the implementation of a certain degree of data localization measures, and in most cases, China still restricts and limits data flows with localized data storage. Although data localization is certainly conducive to safeguarding citizens’ personal information security, creating a good
environment for the development of China’s data industry, and maintaining China’s data security and national security. Data localization is not suitable any more for securing China’s data in the complex and changing international situation, while in the context of the globalization of the digital economy, strict data localization measures will instead hinder the cross-border flow of data and the sustainable development of the digital economy.

The data localization measures currently implemented in China do have certain shortcomings. First, data localization cannot reflect the value of data. The cross-border flow of data has become a major engine of global economic growth, while restricting or prohibiting the cross-border flow of data is tantamount to hindering the development of the global digital economy (Cheng, 2018). Moreover, data are an aggregated resource, of which the value needs to be realized through data sharing. In turn, the sharing of data must allow data to flow across borders, and only data that flow can truly realize its value. In other words, data localization leads to the restriction of cross-border flow of data, which hinders the realization of data sharing and prevents the value of data aggregation.

Second, adopting data localization measures will not help maintain our data sovereignty. The idea of maintaining data sovereignty by fixing the location of data storage and by restricting the flow of data across borders does not hold water; the maintenance of data sovereignty does not depend on the location of data storage, and highly centralized data are instead more vulnerable to attack or destruction (Bauer, 2017). Thus, data localization is not ipso facto more conducive to preserving data sovereignty than the cross-border flow of data, and data localization measures do not have the desired effect on preserving data sovereignty.

Jurisdictional level: China’s data sovereignty jurisdiction principle is mostly reflected in unilateral perspective. At present, China’s jurisdiction over data is centered on data localization, coupled with restrictions on outbound data like security assessment, the country mostly takes the government as the main regulatory body and controls data flow in one direction. This ignores the dynamism of personal data and enterprise data, deprives individuals and enterprises of their data empowerment, which is not conducive to stimulating the vitality and potential of cross-border data flow.

One-way government control of data may also lead to an overly rigid data governance system, which is not helpful to realizing the economic benefits of data in the era of globalization of the digital economy, nor is it beneficial to promoting two-way data flows and international cooperation of data jurisdictions. Such a stagnant control approach will only make data economically worthless and even make our country develop into a data isolation, gradually losing the economic value brought by data flow, while ultimately failing to balance the maintenance of data sovereignty and economic interests from data.

International level: Less participation in the development of international rules on data sovereignty. Compared with the active performance of the U.S. and Europe in the institutional design and international making of data sovereignty rules, China has been less involved in the process of. For example, in the Organization for Economic Cooperation and Development, the main multilateral mechanism for global data governance, coordinating the rules for cross-border data flows, of which China is still not a member. As a country with a huge data flow, there are no bilateral or multilateral agreements involving data rules in our country yet. This constrains our voice in the data field and makes it difficult for us to have international influence on the rules of data sovereignty (Huang & Wei, 2021).
Although CPTPP is the most comprehensive and the highest level of agreement in the world, it retains most of the contents of TPP in terms of cross-border data flow, which to a certain extent still reflects the attitude of the U.S. towards cross-border data flow (Yu & Jiang, 2021). Currently, the CPTPP is dominated by Japan, which is opposed to China’s application to join, and Japanese Prime Minister Yoshihide Suga has publicly questioned whether China’s existing legal system meets the high standards of the CPTPP rules. On September 27, 2021, Australian Trade Minister Dan Tehan also publicly stated that Australia was opposed to China joining the CPTPP.

It can be seen that China regulates the cross-border flow of data based on the Cyber Security Law and the Data Security Law, but lacks a systematic regulatory system and clear rules of data sovereignty. And at this stage, China, as a big country in data production and application, should actively safeguard our data sovereignty, participate in the formulation of international data sovereignty rules, and compete for the right to speak about international rules in the data field.

**The Policy of Constructing Data Sovereignty Rules in China**

**The Concept of Building China’s Data Sovereignty Rules: Seeking a Balance Between Data Protection and Data Openness**

The core element of data sovereignty is the issue of the relationship between data and sovereignty, i.e., the exercise of data sovereignty requires seeking a balance between data protection and data openness. In the field of data sovereignty, two competing and intertwining perspectives on the relationship between data and sovereignty have emerged: data protection and data openness (Zhang, 2020). Data protection advocates that the cross-border flow of data should be regulated by data sovereignty, while data openness advocates that data should flow freely across borders without sovereign interference. Data protection emphasizes the control of data and pays more attention to data security; while data openness emphasizes the flow with sharing of data and pays more attention to the freedom with economic benefits of data. Data protection and data openness have always been the contradictory points in regulating the cross-border flow of data, in which we cannot advocate data protection merely based on data sovereignty, nor can we talk about data openness in isolation from data sovereignty. Maintaining data sovereignty is a prerequisite for data openness, considering that data sovereignty is the foundation, data protection is the political goal, and data openness is the development goal. No country will choose to give up data sovereignty without data protection and simply open up data sharing, but no country can give up the economic benefits of open data either. Therefore, this country should give full play to the necessary modesty of data sovereignty, avoid overly rigid fixation, and reject absolute control of data sovereignty. Of course, it should also prohibit the cross-border flow of data that violates data sovereignty, and for avoiding data sovereignty disputes, we should promote the effective use of data resources by the principle of data openness.

**Establishing Data Sovereignty Jurisdiction Rules**

First, the jurisdictional principles applicable to data sovereignty should be determined. This country applies the jurisdictional rule of territoriality as the main principle while personal and protective regulations as the supplementary principle, and has jurisdiction over all persons and properties within the territory. But traditional jurisdiction can no longer solve the problem of borderless space in the field of virtual data. Therefore, in the field
of data, China should supplement the principle of effect jurisdiction to the one of traditional jurisdiction (Svantesson, 2014). A state is entitled to exercise jurisdiction when activities occurring outside its territory cause injurious consequences to that state. The principle of effect breaks the limits of territorial jurisdiction, while blurs the line between territorial and extraterritorial jurisdictions.

Second, the scope of extraterritorial jurisdiction should be expanded in the data sovereignty rules. Since data is naturally mobile, China must consider the issue of extraterritorial jurisdiction over data in order to maintain data sovereignty. From the international perspective, the expansion of data jurisdiction is an inevitable trend. Therefore, when establishing data sovereignty rules, China should reasonably define the boundaries of data jurisdiction. Before which it should be clear that the independence of data sovereignty is relative and differs from the complete, absolute and independent character of traditional state sovereignty. In practice, the repeatability of data leads to the fact that data sovereignty can be possessed by multiple subjects; at the same time, data may also flow in multiple countries or regions, which may be stored in multiple countries or regions. There may be two or more countries asserting sovereignty over the same data at the same time, leading to a conflict of jurisdiction over the cross-border data flows. Such conflicts result in the inability of any one country to exercise data sovereignty independently and fully without regard to the data sovereignty of the other (Zhai, 2018). There may also be situations where multiple states or multiple enterprises asserting authority over the same data at the same time, given the flow and storage of data is often controlled by the enterprise, and the state controls the data by controlling the enterprise. That is, not only can states assert data sovereignty, but enterprises can also assert control over data. Therefore, the maintenance of data sovereignty by the state is not only subject to the constraints of international law, but also is limited by the data sovereignty of other countries or enterprises, as a result data sovereignty no longer has the absolute and exclusive nature of traditional sovereignty.

Finally, in order to better safeguard data sovereignty, China should attach importance to the construction of key data infrastructure through legislation, timely updated physical equipment, such as software and hardware, promoting technological innovation, independent research and development, as well as ensuring the environmental security of data in the whole process of cross-border flow.

**Determine the Reasonable Scope of Applying Data Localization**

The Group of Twenty (G20) Digital Economy Ministerial Meeting in 2020 emphasized that cross-border data flows should aim at a win-win cooperation and cross-border coordination of data from member states. Data localization, as a regulatory measure for cross-border data flows aiming to restrict data flows, is regarded as contrary to the trend of globalization of digital economy and cross-border data cooperation. According to the strength of data localization, it can be divided into: (1) absolute data localization, i.e., data can only be stored and utilized within the country, and all cross-border data flow behaviors are prohibited, completely negating the economic value generated by data flow; (2) relative data localization, i.e., allowing eligible foreign providers of data service or foreign governments to access data stored in their own countries. This kind of data localization does not completely prohibit the cross-border flow of data, but rather conditionally allows a certain degree of data openness on the basis of maintaining the country’s data sovereignty and digital economic value. This kind of data localization is relatively regulated, and it is the very approach that applies to this country; and (3) localized data backup, which only requires data to be backed up within the country, so that the data can be readily processed and
utilized, without any other restrictions, while the backed up data can flow freely across borders (Huang & Hu, 2019). This kind of data localization not only facilitates the processing and utilization of data in the home country, but also prevents important data from leaving the home country by means of keeping the backup, balancing the efficiency of data utilization in the home country and the value brought by the cross-border flow of data, which is the future development direction of data localization. China should adopt different types of data localization for different data according to its classification and grading, in order to balance data localization measures and to take into account data security with economic benefits.

This country should back up all types of data, because whichever type, which may involve economic interests or national security, is all of protection significance. At the same time, localized data backup can make the use of data more convenient, which can be retrieved, analyzed and processed at any time; this is conducive to the control of data and to the maintenance of data sovereignty in China. For general data, localization backup should be adopted to allow free cross-border flow of them; for critical data, relative localization should be adopted to allow cross-border flow of them under the premise of ensuring their security. For sensitive data, absolute localization should be adopted to strictly control the cross-border flow of them, so as to prevent the security of national data from being infringed.

We should recognize that the free flow of data across borders is the general trend, and restrictions on it can only be relative. Therefore, China should prohibit the application of absolute localization to data across the board, and instead determine different types of data localization based on different categories and levels of data.

Active Participation in International Legislation on Data Sovereignty Rules

In 2019, China already accounted for nearly a quarter of the global cross-border data flows and was growing at an average annual rate of 3% faster than the rest of the world, which was expected to have the world’s largest data circle by 2025. As a digital economy powerhouse and a large country with huge cross-border data flows, China should build up confidence in leading the rule-making of data sovereignty, strengthen international cooperation on data sovereignty rules, and build an open, inclusive, mutually beneficial ecosystem of data cross-border flow. China should become an important participant in improving international coordination on cross-border data flows, while cooperate with various countries, regions and international organizations to promote the signings of bilateral and multilateral agreements on international rule-making of cross-border data flows (Liu, 2020). To achieve such, it is necessary to reach a consensus on data sovereignty among the participating countries, and the sovereignty of each country in the field of data should be protected. China should seize the chance to respect the data sovereignty of all countries, take advantage of the “Belt and Road” initiative and the “Digital Silk Road”, while regarding the signing of the RCEP as an opportunity, China should also strive to sign bilateral and multilateral agreements on cross-border data flow with its important trading partners as well as promote the establishment of new international rules on data sovereignty (He, 2021). In 2020, China proposed the Global Data Security Initiative to create a secure and fair development environment for data flows across borders. This not only maintains global data security, but also contributes Chinese wisdom to the international rules of data sovereignty.

In addition, the rampant epidemic has sent shockwaves through the global economy, yet it has also given another opportunity for further development of cross-border data flows. This country was the first to recover
from the epidemic, but the situation for the rest of the world is still very serious. In the era of digital globalization, this country can hardly be left alone. Relying on its long-accumulated technological advantages in the digital economy, China should play its role as a digital power, provide a prudent and inclusive Chinese solution to global data sovereignty rules and cooperation, while enhance the international influence of China’s data sovereignty.

**Conclusion**

In order to compete for dominance in the data field, the U.S., Europe and Russia have all formulated relevant rules and development strategies, which has intensified the competitions of data sovereignty among countries. As a major country in data origin, flow and application, China should actively respond to the layout of data sovereignty by data powers, like the U.S., Europe and Russia on the one hand, while face up to the imperfect status quo of data sovereignty rules in China on the other. With the development of digital globalization, the risk caused by the lack of data sovereignty rules is becoming increasingly serious. China needs to adapt to the changes of the times, accelerate the construction of data sovereignty rules, safeguard our national security and national interests, while provide Chinese solutions for global data governance and international rules of data sovereignty.

**References**

Bauer, T. (2017). The cost of data localization: Self-defeating behavior during economic recovery. *Journal of Shantou University (Humanities and Social Sciences Edition),* 5, 44-47.

Cheng, X. (2018). On personal data rights in the era of Big Data. *Chinese Social Sciences,* (3), 108-122.

Ding, X. D. (2018). What are data rights? The protection of data privacy from the European “General Data Protection Regulation”. *Journal of East China University of Political Science and Law,* (4), 39-55.

He, A. J. (2021). The confrontational posture of data globalization and data sovereignty and China’s response—An analysis based on the perspective of data security. *Journal of Beijing University of Aeronautics and Astronautics (Social Science Edition),* 34(3), 18-26.

Huang, D. L., & Hu, W. H. (2019). The basic pattern of global data localization and cross-border flow legislation regulation. *Information Security and Communication Privacy,* (9), 22-28.

Huang, H. Y., & He, M. T. (2019). An interpretation of the U.S. data sovereignty strategy based on the CLOUD Act. *Journal of Information Resource Management,* 9(2), 34-45.

Huang, Z. X., & Wei, X. Y. (2021). The US-EU cross-border data flow rules game and China’s response—A perspective on the invalidation decision of the privacy shield agreement. *Journal of Tongji University (Social Science Edition),* 32(2), 31-43.

Jiang, Z. D. (2021). The EU’s construction of digital: The logic of “sovereignty” and China-EU digital cooperation. *International Forum,* 23(4), 64-80.

Jiménez-Gómez, B. S. (2021). Cross-border data transfers between the EU and the U.S.: A transatlantic dispute. *Santa Clara Journal of International Law,* 19(2), 1-45.

Liu, T. J. (2020). The theoretical divide and practical conflict between data sovereignty and long-arm jurisdiction. *Global Law Review,* (2), 180-192.

Orlova, A. V. (2020). “Digital sovereignty”, anonymity and freedom of expression: Russia’s fight to re-shape Internet governance. *UC Davis Journal of International Law & Policy,* 26(2), 225-247.

Sun, N. X., & Zhang, X. J. (2015). On data sovereignty—An examination based on virtual space games and cooperation. *Pacific Journal,* 2(2), 63-71.

Svantesson, D. J. B. (2014). The extraterritoriality of EU data privacy law—Its theoretical justification and its practical effect on U.S. businesses. *Stanford Journal of International Law,* 50(1), 53-102.

Wang, Z. Y., & Liu, Y. Y, (2020). The “Sovereign Internet Act” and the practice of Russian cyber sovereignty. *Information Security and Communication Secrecy,* (10), 93-99.

Xu, K. (2021). Freedom and security: A Chinese solution for cross-border data flows. *Global Law Review,* 43(1), 22-37.
Ye, K. R. (2020). “Long-arm jurisdiction” in the regulation of cross-border data flows: A fundamentalist examination of the EU GDPR. Law Review, 1(1), 106-107.
Yu, M. J., & Jiang, H. W. (2021). From RCEP to CPTPP: Differences, challenges and countermeasures. International Economic Review, (2), 129-144.
Zhai, Z. Y. (2018). The rise of data sovereignty and its dual attributes. China Law Review, (6), 196-202.
Zhang, C. H., Cai, R. Y., & Zhang, L. K. (2017). Review and insights on network information security strategies of major developed countries. Modern Intelligence, 32(1), 172-177.
Zhang, X. J. (2020). Patterns and lessons learned from the rule building of data sovereignty—Also on the rule building of data sovereignty in China. Modern Jurisprudence, 6(6), 136-149.
Zhou, Y. (2020). The risks of social co-governance of public information services and its control. Intelligence Information Work, 41(1), 69-78.