Regulatory Approaches of Cross-border Data Flow in the Big Data Era: China’s Choice

Xi Yang
Department of Law, Xi’an Jiaotong University, Xi’an 710049, China
yangxi@xjtu.edu.cn

Abstract. Cross-border data flow is characterized by multi-direction and rapid dynamic gridding in the big data era. Accordingly, these characteristics necessitate effective regulation for cross-border data flows. The US and the European Union (EU) follow their respective regulatory models for cross-border data flows by considering each one’s economic, political, and historical traditions. The “geographically based” policy of data flows, characterized as internal and external, is the basic position adopted by the EU on cross-border data flows. Although the US regulatory path favors (in principle) the free flow of data across borders, this country actually adopts data protectionism for data involving critical technologies and security areas. Given the political system differences among China, the EU, and the US, China can learn from the experiences of the US and the EU, actively seek value balance between data regulation and free flow, construct its own regulatory model, and establish a diversified data management system. Lastly, China should also actively participate in the international regulation competition on cross-border data flows, thereby giving the country a voice in the international arena.

1. Introduction

The big data era is an information age built on modern network information systems, such as the Internet and Internet of things. Numerous data resources are widely collected, stored, value extracted, intelligently processing, and displayed in this era. With the rapid development of a new generation of information technologies, such as the Internet, cloud computing, and artificial intelligence, in the big data era, the multi-directional and dynamic networking of data flow has gradually emerged under the impetus of science and technology. In the big data era, large-scale and complex data flow have become considerably easy and convenient, and cross-border data flow has become the growth engine in a new round of globalization. Therefore, the total scale of the global digital industry has exceeded millions of billion in 2019, among which China, the US and the EU have obvious advantages (in table 1).

| Countries | Total scale of digital industry | Growth (%) |
|-----------|--------------------------------|------------|
| China     | 2566990                        | 14         |
| US        | 1902037                        | 9.5        |
| EU        | 321541                         | 10         |

Although data flow creates enormous economic wealth and social value, cross-border data flow is not consistently orderly and safe. That is, disorderly data flow may pose serious challenges to national security interests, regulatory frameworks, and even law enforcement. For reasons of data privacy...
protection, national sovereignty integrity, and security, some countries have restricted cross-border data flows by enacting policies, laws, and regulations. For example, the EU and the US have regulated cross-border data flows. The two regulatory models they have created lay the foundation for the international pattern of cross-border data flows. Despite the enactment of the “Cybersecurity Law of the People’s Republic of China” in 2017, China has yet to establish an effective regulatory system for cross-border data flows.

Therefore, this study focuses on the regulatory approach of cross-border data flows in the big data era. First, this research defines the new characteristics of cross-border data flow in the big data era. Second, the current study discusses the different regulatory approaches in the field of cross-border data flows in the US and EU, and summarizes the characteristics of the two regulatory models. Lastly, by identifying the shortcomings of the cross-border data flow regulatory system in China, this research proposes some suggestions on establishing a regulatory system for cross-border data flow in this country in the future.

2. Characteristics of cross-border data flow in the big data era

2.1. Multi-directional data flow
Cross-border data flow refers to the flow of data among different jurisdictions. \(^2\) The concept was first proposed by the Working Group on Computer Applications (CUG) under the Organization for Economic Co-operation and Development (OECD) Committee on Science and Technology Policy (CSTP) in the 1970s. \(^3\) Cross-border data flows in the late 20th century were dominated by “point-to-point” data exchange model. The main body of data processing is clear, the process is distinct, and the number of data flow is limited and scattered (e.g., exchange of business data among several companies in different countries). However, in the big data era, large-scale and complex data flows across borders have become the global norm. Data acquisition, analysis, and processing are no longer one-way processes. Data flow from the starting to the end points will go through multiple subjects and links. Moreover, the flow frequency will become real-time and continuous. Therefore, in the big data context, the process of data searching and extraction has changed fundamentally. \(^4\) The simple “point-to-point” data exchange model has been transformed into a multi-agent, multi-link, and multi-direction real-time continuous flow.

2.2. Dynamic gridding of data flow
Data are traditionally prepared before they move across borders, and transported from origin to destination through defined transit mechanisms in a predictable manner. However, the progress of information technology (IT) in the big data era has resulted in the increasing maturity of the global system of data identification and division. That is, cross-border data may be identified, captured, and processed by data processing organizations at any time in the flow process. Moreover, the approach of cross-border data flow is no longer fixed. Therefore, the dynamic, unpredictable, and uncertain data flow network has become the characteristics of cross-border data flow in the new era.

3. Regulatory approaches for cross-border data flow in the big data era
The multi-direction and dynamic gridding characteristics of data flow has led to an increasing convenience in acquiring remote data. Even if data are stored locally, nothing can prevent the remote unauthorized access to data. Given the concerns with the dangers to national security and public interest of an unsafe data flow, the international community has sought to regulate cross-border data flow. \(^5\)

As can be seen from Figure 1, since 2000, the promulgation and revision of data laws have increased significantly. Especially after 200 data laws were amended in 2014, the number of revisions and promulgations of relevant data laws has increased exponentially each year. At present, the US and the EU are two leading forces in the field of cross-border data protection, but their regulatory models are considerably different from each other.
3.1. EU supervisory approach: Dual supervisory approach based on geography
The EU adopts a “geographically based” approach to regulate cross-border data flows. That is, impeding the free flow of cross-border data on the grounds of data protection is forbidden within the EU member-states. By contrast, other “third countries” (i.e., non-member states) need adequate protection of data flows. [6]

3.1.1. Free data flow within the region
Within the EU member-states, Article 12 of the “Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data” (hereinafter referred to as “the Convention”) enacted in January 1981 stipulates that state parties cannot restrict cross-border data flows solely on the ground of protecting privacy. That is, data can be moved within the EU member-states as long as they provide “the same level” of protection.

In October 1995, the EU issued “Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data” (hereinafter referred to as “the Directive”), which is the core standard of the EU data protection. On the basis of “the Convention” to reduce the obstacles to data flow caused by domestic laws in member countries, “the Directive” further enhanced data mobility within the EU. Moreover, “the Directive” draws on and integrates the legislative practice of various European countries in terms of the rights and obligations of data controllers, data supervision, and other contents. The practices of reducing barriers and seeking free flow reflect the requirements of political and economic integration within the EU, and also indicate that the EU’s internal regulatory position is considerably inclined to encourage data flow. [7]

3.1.2. “Sufficient protection” principle of data flow outside the region
The EU applies the “sufficient protection” principle when data are transferred outside a member-state. “The Directive” states that data can be transferred only when third countries provide “similar,” “equivalent,” and “adequate” protection to the EU or meet the EU requirements. Moreover, the “General Data Regulation Protection (GDPR)” of the EU, published in May 2018, presents three criteria for assessing whether third countries provide specific adequate protection: (1) rule of law, including the degree of respect for human rights and fundamental freedom, as well as the relevant comprehensive and specialized legislations and their implementation; (2) existence of a specialized regulatory organization that operates effectively; and (3) acceding to international treaties or multilateral agreements on the protection of personal data, thereby assuming obligations under international law in that field. [8] In addition, GDPR is covered if personal data in the EU are used or processed by data institutions in providing products and services. Such an extensive extraterritorial jurisdiction strengthens the EU’s data control. The EU can be considered to be markedly inclined to data restriction and control in terms of data flow outside.
The position of “geographically based” distinction between internal and external data flows is an effective attempt of the EU to seek how to protect data security while promoting data flows. [9] This regulatory path unifies standards, provides reasonable expectations for the realization of data rights, and facilitates the prevention of third countries from circumventing their own data protection legislation. [10]

### 3.2. Regulatory approach of the US: Principle of accountability as core

#### 3.2.1. Free flow of data and accountability system after the fact

The leading role of the US in the fields of digital economy and IT is the objective basis and premise of its policy of advocating the free flow of global data. [11] As an Internet power, the US has established an approach of emphasizing the free flow of data while disregarding government control at the initial stage of promoting cross-border data flow. [12] By setting privacy protection standards in the American industry, the default data controller or processor can consciously abide by the relevant rules in business activities, and be responsible for the security of data in a legal and reasonable manner. Accordingly, only when data controllers or data processors commit violations in cross-border data flows can data regulators punish them. On the one hand, the data regulation approach in the US evidently relies on enterprises’ conscious compliance with data rules. On the other hand, such an approach emphasizes the accountability of enterprises when they violate the rules. This regulatory approach provides a minimum standard for the digital economy industry and cross-border data flow, bringing the restriction mechanism of cross-border data flow back to the market.

#### 3.2.2. Regulate data involving key technologies and security

In recent years, the US has tightly restricted the cross-border transfer of technical and sensitive data involving major science and technology fields. For example, the US Export Administration Regulations (EAR) signed by the US in August 2018 stipulates that export control is not limited to “hardware” exports but also includes “software.” That is, the transfer of scientific and technological data to servers outside the US or data out of the US must obtain an export license from the Department of Commerce Bureau of Industry and Security. In terms of foreign investment reviews, the Foreign Investment Risk Review Modernization Act (FIRRMA) stipulates that certain non-controlled foreign investments made by US companies involving “critical technology,” “critical infrastructure,” and “critical or sensitive data” will be covered by security reviews. In addition, the US has expanded the scope of data regulation through “long-arm jurisdiction.” In March 2018, the US passed the “Clarifying Lawful Overseas Use of Data Act (Cloud Act)”, which stipulates the principle that “whoever owns the Data owns the control of the Data.” This principle breaks the old “server” standard and implements the “data controller” standard, which allows the government to access and monitor data across borders.

In principle, although the US regulatory approach tends to promote the free flow of cross-border data, it adopts data protectionism for data related to key technologies and security areas. Although the US hopes to promote the free flow of data and build a barrier-free global Internet system, it is likewise wary of the potential threat posed to its dominant position, particularly by the emergence of Internet companies in China and India.

### 3.3. Regulatory features of cross-border data flow in the big data era

Although the EU and the US have differences in the regulatory paths of cross-border data flows, the two regulatory methods also have some similarities in the big data era.

#### 3.3.1. Focus on national data security

Data in the big data era contain huge economic and strategic value. [13] Data are no longer important assets only for enterprises but also a strategic resource for countries. In particular, data of individuals, enterprises, and other entities are the embodiment of countries’ “soft power” and also related to the military and national defense. Therefore, data are significant to the maintenance of national sovereignty. Data are likewise a strategic resource to support national security and development, and have immense
value in terms of protecting sovereignty. [14] Another inevitable demand of regulatory legislation in the big data era is realizing the coordinated development between the free flow of data across borders and national security. Therefore, the increasing free flow of data at present has resulted in the close linkage between data regulation and national security. Accordingly, important scientific, technological, and national security data have become significant objects of supervision.

3.3.2. Expand jurisdiction
In recent years, an increasing number of countries have been competing for data resources around the strategic game in cyberspace. The EU has built a strong legal framework in the field of data flow-GDPR. This legal framework applies to natural persons, data processing operations, and personal data within the EU, and also extends these standards outside the EU. An example is the historic “Google data privacy case” in 2014. GDPR indicated that as long as Google provides services or conducts regulatory activities for data users in the EU, GDPR remains binding even if Google refuses to comply with the EU regulations on the ground that the company does not have data controllers and processing agencies in the EU.

The US “Cloud Act” has similar provisions. This law provides the US government legal authority to retrieve data stored in other countries. The Cloud Act also allows the exchange of data between the US and other countries if they reach an “agreement” on the flow of data. Accordingly, the US created a regulator that can bypass countries where data are located, thereby extending US enforcement to these states.

4. Approach selection of cross-border data flow regulation in China
The White Paper on the Development of Digital Trade (2020), which was released by the China Academy of Information and Communications Technology, indicated that the added value of the Chinese digital economy in 2019 reached 35.8 trillion yuan, accounting for 36.2% of the GDP and 7.85 percentage points higher than the nominal GDP growth in the same period. [15] Thus, the position of the digital economy in the national economy has been further highlighted. Despite the increasing size of the digital economy, China continues to have problems in cross-border data flow.

4.1. Existing problems of cross-border data flow regulation in China

4.1.1. Lack of systematic legal norms
In general, laws on cross-border data flow in China lack detailed provisions with strong system and procedures, which are scattered among various laws, regulations, and department regulations. Moreover, the existing laws and regulations on cross-border data flow are mostly restrictive in nature, and their overall orientation adopts “data sovereignty” and restricts the transfer of domestic data to foreign countries. For example, the “Guidelines on the Protection of Personal Information in Information Security Technology Public and Commercial Service Information Systems,” which was issued by the Ministry of Industry and Information Technology in 2013, formulated relevant provisions on cross-border data flow for the first time. However, the contents were only relatively principled, and only a few provisions focused on data subject rights, regulation methods, and relief approaches. In June 2017, the “Cybersecurity Law,” which is the basic law on cyberspace security management in China, came into effect. This law defines China’s basic policies on cross-border data flow and establishes a basic legal system in this field for the first time. However, laws and regulations on cross-border data flow have yet to be passed, and the mechanism of data evaluation and regulations on data localization has remained vague. Consequently, this decentralized and abstract legislative model cannot provide a stable legal basis and guarantee for the rapid development of cross-border data flow.

4.1.2. Ambiguity of attributes and types of data rights
At present, the legal field in China is divided on the issue of personal data ownership. One view is that personal data contain information that is personal nature, thereby attributing data to the category of
privacy or personality rights. The other view is that the law gives the data subject the right to know, control, and dispose data, thereby making personal data a property right. Consequently, this ambiguity will hinder the future regulation of data markets. In addition, China defines data types broadly. At present, Chinese legislations do not clearly stipulate an effective data type recognition system, and have yet to form the overall mode of differentiated management for different types of data and performance. The same level of data protection disregards discrepancy in different types of data.

4.1.3. Single supervision method

The supervision of cross-border data flows in China is generally government-led. However, the Chinese government is currently overburdened with regulating cross-border data flows, thereby inhibiting market efficiency. Moreover, the consequence of heavy government supervision is that enterprises bear minimal regulatory responsibilities and the internal self-discipline of each industry is relatively weak. Chinese legislations on cross-border data flow are relatively late, and considerably principled in terms of legislative mode, system, value orientation, specific rules, and implementation and relief mechanisms. Therefore, cross-border companies cannot adjust their cross-border trading behaviors based on legitimate and reasonable expectations.

4.2. Approach selection of cross-border data flow regulation in China

At present, the regulatory approaches of the EU and the US on cross-border data flows represent two modes of international supervision of cross-border data flows. On the one hand, the EU emphasizes control and strict supervision of data flows outside the region. On the other hand, the US places considerable emphasis on the free flow of data. Given the political system differences between China and the US and the EU and the imperfect legislations on cross-border data flow in China, China cannot fully accept the data governance model of the EU and the US. Hence, China should opt for the right path based on its actual situation and the development trend of cross-border data flow.

4.2.1. Seek value balance between data regulation and free flow

The big data era emphasizes the rational development and utilization of data. The single pursuit of the strict protection of data or unlimited free flow is inconsistent with the requirements of the big data era. Although laws require necessary restrictions and security assessments on the operation and flow of data, the ultimate goal of legislations should be to promote the free flow of data in accordance with laws and order. Only when data are circulated in a safe and stable environment can data operators substantially develop and utilize data. Moreover, clarifying and refining the conditions of data flow will enable data operators to easily judge the boundaries of the flow of data. Therefore, China can open its digital market and conduct digital trade on the premise of clarifying the open scope of the cross-border flow of international data and ensuring personal privacy and data security. Moreover, the orderly and effective regulation of cross-border data flows in China will enable the Chinese data regulatory system to “go to global” and align with the current relatively mature international rules. Otherwise, the recognition and acceptance of the international community will not be satisfactory when large gaps remain in China’s relevant domestic rules.

4.2.2. Establish diversified data management system

With the continuous expansion of the depth and breadth of global data transactions, the single data management model is difficult to adapt to the current development momentum of cross-border data flow and integration. The practice of treating data differently in the EU “Regulation on the Free Flow of Non-Personal Data” shows that the management mode of data classification and refinement has been initially applied and is likely to become the development trend in the future. Therefore, China can continue to refine data types and adopt various management models for different data. For example, Article 14 of the GATS Privacy Exception and the National Security Exception Clause indicates that data involving state secrets and national security shall be retained in China. By contrast, ordinary personal data can be divided into general and sensitive data. Meanwhile, government public data are related to the public
welfare and publicly availability because these data consider public service functions, such as citizen data information management and e-commerce construction. Thus, opening government public data can improve the ability of countries’ governments to manage public information. Moreover, the transaction of public data under the condition of ensuring security can serve the public and generate additional value. To this end, China should actively establish a diversified cross-border data management system to maximize the value of data by making the best use of different data.

4.2.3. Strive for the international discourse power of cross-border data flow regulation
Cross-border data flows, which underpin the development of global digital trade, have a natural “global nature.” Therefore, the rules that govern data flows across borders must also be based on a global perspective. At present, the EU and the US have formed an international regulation leading system on cross-border data flows, which have a wide and far-reaching impact on the global scope. By contrast, China has no specific legislation on cross-border data flows, and no multilateral negotiations on cross-border data flows with the EU and the US. Evidently, China has been relatively passive in the international regulation of cross-border data flows. Therefore, China should actively engage in bilateral or multilateral negotiations with the EU and the US on cross-border data flows, and participate in the discussion and formulation of international rules. As an Asia-Pacific Economic Cooperation (APEC) member and promoter of international trade, China should substantially contribute to personal data protection and cross-border data flows.

5. Conclusion
Cross-border data flows are becoming an important feature driving the new globalization. The influence of such factors as geopolitics, national security, privacy protection, and industrial development level has prompted different countries to adopt various regulatory models to construct cross-border data flows. Given China’s political system differences with the EU and the US, as well as status of a developing country, China can actively seek value balance between data regulation and flow, construct its own regulatory model, and establish a diversified data management system by learning from the experiences of the EU and the US. Lastly, China should take the “One Belt and One Road” initiative as an opportunity to actively participate in international regulatory competition by developing a cross-border data regulatory system with Chinese characteristics. In this manner, China’s voice will be enhanced and heard internationally.

Acknowledgments
The author is most grateful to the Law School of Xi’an Jiaotong University. The research is funded by the projects of National Social Science Foundation of China Youth Project: Multilateral Reform and Chinese Countermeasures of International Investment Arbitration under the Background of "One Belt and One Road" (Project No.:18CFX084)

References
[1] Jia Kai. (2017) Conflict and cooperation: evolvement of trans-border data flows between US and EU[J]. Journal of Shantou University (Humanities & Social Sciences),33(5):57-64.
[2] Christopher Kuner. (2013) Trans-border data flows and data privacy law[M]. Oxford University Press, 11.
[3] G. Russell Pipe. (1984) International information policy: evolution of trans-border data flows issues[J]. Telematics and Informatics,1(4):409.
[4] Huang Daoli, He Zhile. (2017) “Big data phenomenon” of US and EU data cross-border regulation legislation and enlightenment for China[J]. Journal of Intelligence, 36(4):47-53.
[5] Shi Yewei. (2020) International trade rules in cross-border data flows: regulation, compatibility and development[J]. Journal of Comparative Law, (4):173-184.
[6] Liu Hongsong and Cheng Haiye. (2020) Global governance of transborder data flow: progress, trends, and China’s path[J]. Global Review,12(6):65-88.
[7] Yang Xi. (2019) Intergenerational development and experience of EU's personal data protection system —a model of internal regulation and external expansion[J]. International Business, (5):145-156.

[8] Article 45(2) of the 2016 General Data Protection Regulation.

[9] Kuner C. (2010) Regulation of transborder data flows under data protection and privacy law: past, present, and future[R]. OECD Digital Economy Papers,20-21.

[10] LI Yanhua. (2019) Regulation path and China's choice on global cross-border data[J]. Present day Law Science,17(5):106-116.

[11] Zhang Monan. (2020) Cross-border data flow: global situation and the countermeasures for China[J]. China Opening Journal, (2):44-50.

[12] Zhang Sheng. (2019) The international law regulation path of cross-border data flows by the United States and China’s countermeasures[J]. Business and Economic Law Review, (4):79-93.

[13] Knoke D. (2015) Emerging trends in social network analysis of terrorism and counterterrorism[J]. Emerging Trends in the Social and Behavioral Sciences: An Interdisciplinary, Searchable, and Linkable Resource,1-15.

[14] Cheng Xiao. (2019) Personal data rights in the era of big data[J]. Social Sciences in China,40(3):174-188.

[15] China Academy of Information and Communications Technology. (2020) White paper on the development of digital trade (2020). http://www.caict.ac.cn/english/research/whitepapers/202012/t20201228_367176.html

[16] Huang Ning, Li Yang. (2017) The evolutionary trend of trans-border data flows regulation and its cause analysis[J]. Journal of Tsinghua University (Philosophy and Social Sciences),32(5):172-182.