Governance in the Free Cross-border Flow of Data

Yuqian Lyu*

Department of Law, University of Exeter, Exeter, England

*Corresponding author: yl1010@exeter.ac.uk

Abstract. Every part of life, work and friendship has been inseparable from the Internet. When we casually click on the links on the network, when we need to enter personal information on the network due to work and policy, when enterprises are used to storing most of the data in the emerging cloud computing service platform, when the official website of the core departments of the country was maliciously attacked. We are facing more frequent information leakage in the era of big data. Especially with the trend of multinational corporations, regional interoperability, and the integration of the world economy, data and information can flow across borders without obstacles. Undoubtedly, cross-border business trade, project co-operation, geo-location, and server tracking are necessary, but the large amount of data recording, flow, and tracking brings great risks to personal privacy, business secrets, and the maintenance and stability of national security. As a result of the growing awareness of the risks and drawbacks of cross-border data flows, jurisdictions and regions have developed legislation and rules to balance the free flow of data and cross-border security.

Keywords: Free flow of data; data governance; cross-border; international cooperation.

1. Introduction

As the most central and valuable factor of production in the digital economy, data is gradually a treasured resource and is regarded as the new "oil" or new "diamond" of the business world. Digitalization is spreading throughout the world's economic chain. Cross-border e-commerce has grown 45 times in ten years [1]. According to statistics, two thirds of the world's business activities are now related to digital technologies [2]. Especially some internet company giants such as Meta, Microsoft, Amazon, Google, Apple. They hold a huge amount of data streams and customer information. These data and information are used to provide personalised advertising, upgrade services and gain insight into consumer behavior. However, as the flow of data becomes more widespread, many sensitive pieces of information are more likely to be at risk of being compromised. This is proved by the recent $1.3 billion fine against Meta for violating privacy laws by EU [3]. Particularly when data are transmitted across borders, personal privacy may be violated on a wider scale. Sensitive information such as financial information, health records, family members, etc., once obtained by some criminal organizations, may result in various forms of cyber crime such as identity theft, financial loss and false advertising. In addition, the instability of data and information transmission channels likewise poses a threat to trade secrets. The data leakage in worldwide in 2020 will exceed the total of the last 15 years [4]. In these incidents of information leakage, much sensitive data are involved like government secrets, medical records, and geographic location information. Black trading and malicious theft of information about data are becoming increasingly rampant. Security risks to cloud data or data repositories remain unmitigated. Consequently, laws and regulations regulating the protection of data and information have become a new call in the digital era.

However, as the rules governing the cross-border flow of data information are not uniformly coordinated across jurisdictions, this is clearly a stumbling block for cross-border data information protection. This paper will state the challenges and risks that cross-border flow of data poses to individual privacy and trade secrets and enumerate the current representative regulatory frameworks for data protection. At the same time, it calls for the global establishment of a unified, coordinated and interoperable cross-border data and information management system and the strengthening of international cooperation. The limited and safe cross-border flow of data information is guaranteed.

2. Free Flow of Data

In general, cross-border data flows plays a crucial role in boosting economy, facilitating globalization and encouraging innovation. Supporting the cross-border flow of data reach the the aim for protecting the users' rights and enhance the comprehensive utility of the economy across society. The convenient and instant flow of data makes enterprises to handle directly and efficiently the factor resource in global area. Not only does it support the globalization activities of almost all other factors, including goods, services, capital and talent, but it is also playing an increasingly independent and important role. The potential minimum value of cross-border flows is estimated at US$29.7 trillion over the period 2015-2024 [5]. Cross-border flow of data will bring about a rise in the overall utility of the economy of the whole society, which is important and positive for the economic growth of the country and enterprises. The international movement of data involves the spreading and exchange of information and expertise, and the unrestricted movement of data serves as a significant driver for domestic innovation. As Frost & Sullivan's projected mega trends, data forms the foundation of the future, with 90 percent of revolutionary changes depending extensively on the circulation and utilization of data [6].

However, when large-scale and complex data flows across borders become the common trend, it may pose high risks for individual privacy, trade secrets, national security. The source of the free flow of data is the decentralized and non-geographical modern network structure [7]. Internet without borders may impact the current international order. The importance of data and information determines its high probability of being coveted. The worldwide illicit data industry is maturing rapidly, and there is a frequent occurrence of malicious exploitation and trading of illicitly obtained data. Data leakage is a common occurrence, which not only threatens the privacy and property of individuals, but even concerns their security. At the same time, the importance of data is constantly being highlighted, and data has become one of the key measures of a country's comprehensive strength. These data include not only personal information, but also confidential information of enterprises and the state. This information relates to multiple areas of national security, such as intelligence, military and defence. As a result, data security and mobility have become a crucial part of national security strategies. As states compete for power in cyberspace, the flow and sharing of information is increasingly influenced by political factors. States have begun to demarcate their territories in the emerging cyberspace in order to compete for more power and influence. This has led to more restrictions and controls on the transmission and sharing of information, further deepening the complexity and sensitivity of data flows. Therefore, cross-border data flows are not only about economic and technological aspects, but are also closely related to national sovereignty and security.

3. Cloud Computing and Artificial Intelligence Bring New Challenge to the Data Security

Artificial intelligence, big data, cloud computing, 5G and other new-generation information and communication technologies trigger a new "technological revolution", which is profoundly changing the way in which various industries operate. While bringing new forms of productivity to all areas of society, they have aggravated the security problems of communication networks, such as data leakage, false information and internet extortion. According to a report recently released by IBM, in 2023, the average expense resulting from a data breach has surged to a record-breaking $4.45 million, marking a 2.3 percent rise from the $4.35 million recorded in 2022 [8]. Building a secure and healthy internet and regulatory environment for data flow is a necessity.

Since Open-AI developed and launched ChatGPT, generative AI has introduced more sophisticated threats to internet environments and data security. As an illustration, artificial intelligence has the capability to produce genuine phishing emails, distribute malware, or fabricate convincing deep-fake videos. Studies showcase the simplicity with which credible yet harmful code can be automated at remarkable velocities. With the progression of AI, hackers are expected to discover novel and inventive means to harness its potential for their benefit. They use AI to generate

image videos and web links of fraudulent nature, thus tricking online users into revealing their privacy and even losing their property [9].

For many organizations, the management mostly chooses to store their data in the cloud for the sake of data security. The development companies behind these clouds may be mostly tech giants of multinational nature. This may result in corporate data, secret information from multiple countries (regions) being in the hands of a few techs giant companies. It is difficult not to ensure that the tech companies holding a large amount of data submit information about the collected data to their governments. This is not just a cross-border trade secret leakage crisis, but a possible threat to national security.

For example, an application under IBM called IBM Security® Discover and Classify (ISDC). It allows data search and collection and classification. The main function is to provide real-time, intelligent protection of sensitive data and data tracking for businesses across industries and platforms. The operation of the program relies on scientific and technological techniques such as intelligent algorithms, autonomous machine learning, natural language processing systems, and data analysis to generate an inventory of sensitive data. The enterprise organizations using this procedure inevitably upload all relevant sensitive data to the platform, then the business records, application data of these enterprise organizations are recorded on the backend of the ISDC. Due to the rather broad access rights given to the ISDC when it was initially enabled by the enterprise, the ISDC can even shuttle any data material stored in the enterprise in a state unknown to the enterprise. Because it is only in this way that ISDC can serve its claimed function of protecting and categorizing sensitive data. Furthermore, ISDC supports the data activities of an organization across various platforms. As corporate organizations record their activities on different platforms (e.g. Google, Microsoft, Meta, Amazon, etc.), the volume and variety of data in the cloud keeps increasing and inevitably even crosses national (regional) boundaries. In other words, ISDC can have complete access to sensitive information of business organizations from different countries (regions) and industries. In this case, there must be reasonable and specific regulatory provisions to regulate the flow of data and information records of such programs, as well as the establishment of a solid firewall. This will prevent the malicious theft of large amounts of sensitive information for improper use.

4. The Existing Legal Regulatory Framework：China and The European Union

The trend of free flow of data is unstoppable, but in order to protect personal privacy, commercial secrets, and state secrets, it is necessary to match corresponding policies and regulations to restrict the absolute free flow of data. The European Union and China have both issued documents on regulating cross-border data freedom and safeguarding data security.

4.1. China

On the issue of cross-border flow of data issues, China has not explicitly adopted "data sovereignty", nor has it recognized the attitude of data without borders or complete freedom of data flow. It is only based on the global security concept of risk avoidance [10]. Since 2021, China has successively passed and implemented the Data Security Law, the Personal Information Protection Law, and the Measures for Security Assessment of Data. Dedicated to monitoring and regulating the cross-border flow of private data information and non-personal data information. According to Article 2(2) of the Data Security Law, individuals conducting data processing actions beyond the borders of the People's Republic of China, which result in damage to public interest, national security or the legal rights and society welfare within China, have to subjected to legal investigation and accountability as outlined by the law (and in serious cases, may be investigated refer to the Criminal Law of the People’s Republic of China). This provision suggests that China has recognized the need to expand the scope of regulation of cross-border data flows [11]. However, in determining the geographic scope of what can be regulated, it has to consider the balance between maintaining data

sovereignty and data freedom. On the one hand, it is essential to determine the appropriateness of the extraterritorial application of Chinese data management laws. On the other hand, it is also necessary to consider whether it is enforceable with extraterritorial effect. This is to avoid the dilemma of having rules that can be regulated extra-territorially but not enforced extra-territorially in practice.

Under the existing legal regulatory framework for data and information, the cross-border flow of data is generally unimpeded. However, "data localization" is mandatory for information involving personal privacy, commercial secrets and state secrets. For example, Article 48 of the Law of the People's Republic of China on the Preservation of State Secrets (revised version in 2010), prohibits the transfer of data abroad if it relates to a State secret of China, that only be forcibly stored in China [12]. In the Regulations on the Administration of the Credit Collection Industry, there is also a similar provision. Data amassed by a credit collection agency must be retained within China. If the organization requires the transfer of personal information beyond China's borders, it must adhere to the applicable provisions of laws and regulations [13]. In the Circular of the People's Bank of China on the Effective Protection of Personal Financial Information by Banking Institutions, it regulates that personal financial data gathered within China must undergo storage, processing, or analysis within the country's borders. Unless stipulated differently by additional laws and regulations, banking and financial entities are prohibited from transferring personal financial information abroad from within their jurisdictions [14]. Article 10 of the Measures for the Administration of Population and Health Information stipulates that it is prohibited to store population and health information on servers outside China [15]. Article 34 of the Regulations on the Administration of Maps stipulates that intelligence/electronic map service providers should arrange servers within China for storing map data and establish a security management system and safeguards for Internet map data [16].

According to the Personal Information Protection Law, the transfer of personal information outside the country must only go through the statutory steps and be approved by the Internet Information Office. First, it must pass the information security assessment of the Office of Internet Information Security. Second, certification of personal information protection is obtained through the Office of Internet Information. In addition to the certification, there is also the option of entering into a legally formatted data transfer contract with the offshore recipient of the data. The offshore transmission of personal information requires a complex and rigorous review process. Moreover, the current regulations are not perfect and lack clear case guidance as the implementation period is still relatively short.

In accord with the Data Security Law, Entities or persons within the People's Republic of China are restricted from furnishing data housed within the country's borders to foreign judicial or law enforcement bodies without obtaining authorization from the competent authorities of the People's Republic of China [17]. The "data" here referred to in article 36 includes general data, important data and core data (all data are divided into three categories under the Data Security Law), so the restrictions on the transmission of data outside the country apply to all data under the Law. Similar provisions are also found in Article 41 of the Personal Information Protection Act.

4.2. The EU

The core principle underlying EU regulations for cross-border data transfers is that the right to personal information is an essential human right that necessitates acknowledgment and legal safeguarding [18]. Convention 108, the 1995 EU Directive, the 2016 EU GDPR, and the soon-to-be-considered-adopted Data Act, all of which are EU legislation on the transnational flow of private data information.The Convention108 is the first EU regulatory text to regulate transnational data flows, and it deals only with data flows between European Member States.It provides for European member States to establish their own restrictive regulations on transferring cross-border data. But it does not allow member States to prohibit restrictions on cross-border movement of data completely because of privacy protection [19]. The EU Directive establishes a strict standard of data protection, explicitly requiring that the country of destination of the data flow fulfills the conditions for a level of protection recognised by the EU before digital movement can take place [20]. In order to cope with the huge

impact of the big digital era on personal data protection and to address the gaps in European national legislation that hinder the digital economy, the GDPR was formulated to meet the needs of the European Union. The GDPR is the most standardised and highest level of personal data security protection system in the EU by far.The GDPR has "direct effect" and "primacy" over the laws of Member States, which are required to use the GDPR as a blueprint for the construction of their national regulations, a process overseen by the European Commission.

Not only has it been hugely influential within the EU, but since its adoption, the The GDPR has established a foundational standard for a global surge in data protection laws. Numerous legislators across the world have aimed to align their regulations with the GDPR, with the aspiration of receiving a favorable adequacy determination from the European Commission. Such a determination would enable seamless data exchange between their respective nations and the European market. When companies need to transfer data to countries that do not have an adequacy ruling from the European Commission, the EU obliges those countries to use the Standard Contractual Clauses (SCC) for data transfers under the GDPR to ensure that the rights of EU data subjects are taken into account and upheld. In 2021, the new SCC was approved by the European Commission. On September 27, 2022, the previous SCC was repealed, meaning that on all new contracts entered into after that date must use the new SCC. The complete enactment of the GDPR signifies an unparalleled elevation in the safeguarding and oversight of personal data within the EU. The GDPR is labeled as the most stringent personal data protection act until now.. Any breach of the GDPR will incur a fine of between € 10 million and € 20 million, or between 2% and 4% of a business's global annual turnover, depending on the largest amount.

The regulatory principle of "long-arm jurisdiction" is implicit in the GDPR. This applies not only to organisations processing personal data in the EU, but also to organisations that are not built in the EU with processing activities that involve the provision of goods or services to data subjects in the EU, as well as the surveillance of data subjects. In fact, organisations may be regulated by the GDPR whenever the sale of goods or the targeting of services involves individuals in the EU. In other words, the data subjects who protected by GDPR is individuals in the EU. Individuals, companies or organisations controlling and processing data must have the consent of the data right holder and be able to provide clear evidence of this.

For rules on the cross-border flow of information on non-personal data, the EU has adopted a resolution on the Data Governance Act and is considering the final adoption of the Data Act. These two acts establish a series of strategies for the development of data, including non-personal data. The two bills not only build a regulatory legal structure for the internal flow of non-personal data in the EU, but also close the regulatory loophole for the extraterritorial flow of non-personal data into the EU. This makes the EU non-personal cross-border flow of regulatory rules gradually towards a systematic development path. With regard to the flow of non-personal data within the EU, both acts emphasise the promotion of data sharing within the EU and are committed to enhancing citizens' trust in data sharing.

The legislative objective of the Data Governance Act and the Data Act is to facilitate the flow and sharing of data within the EU. However, there are strict restrictions and scrutiny procedures for data flows outside the EU in both Acts. The most commonly used tool is the stringent "pre-censorship" of data before it crosses borders. Thereby limiting the scope of cross-border flow of data (country). In terms of specific scrutiny requirements, both the Data Governance Act and the Data Act set strict scrutiny standards. For example, assessing whether the level of data protection in certain developing countries meets EU requirements. When an organisation carrying out data storage and processing operations chooses to store or process data and use cloud services in another Member State, the organisation must also comply with all the security requirements applicable to businesses and public administrations in that Member State. The Regulation on the Free Movement of Non-Personal Data has heightened organizations' consciousness regarding their obligations related to the security of data storage and processing across international borders.

5. International Cooperation in Data Security Management

Internet communication itself is characterised by its wide scope, speed and weak sense of boundaries. Coupled with fast-growing technologies such as cloud computing and artificial intelligence, it is not enough to rely solely on the domestic regulation of a particular country (region). Cyber threats and attacks such as hacking, data leakage and cyber espionage do not respect national boundaries. To address data privacy, cybersecurity and potential cyber threats, and to ensure the safe and responsible use of data, it is necessary to establish effective and coordinated international cooperation. By establishing an international cooperation platform, individual countries or organisations are able to share threat intelligence and information on cyber incidents. This facilitates early detection, mitigation and response to cyber-threats.

Moreover, cross-border flow of data involves different countries (regions) in the steps of generation, transfer and use. Each of these steps may suffer to the risk of loss, alteration and falsification.The resulting data sovereignty dispute is a difficult problem that has plagued jurisdictions since the enactment and implementation of data security legislation.Throughout the process of cross-border data flows, it is often difficult to ascertain the attribution of jurisdiction. Coupled with the fact that cross-border data flows have broken through traditional geographical restrictions, the speed of dissemination and geographical span are difficult to control. In dealing with the issue of data security, it is inevitable that the countries involved will have conflicts of legislative jurisdiction, law enforcement jurisdiction and judicial jurisdiction with each other.At present, the world has no unified and coordinated cross-border data security legislation and lacks relevant model cases. Each country or region undoubtedly stands on its own position to ensure that its own interests are maximize. Their assertion of jurisdiction is bound to exacerbate jurisdictional conflicts in the cross-border flow of data. Therefore, the construction of a world-effective regulatory framework to regulate the security risks of cross-border flow of data and information is urgent.

Inter-regional co-operative governance is a good option, as regional regulatory frameworks seem to be easier to develop and implement due to similar geopolitical and legislative concepts. It can also provide empirical solutions for worldwide harmonisation of rules. For example, in the regional agreement of RCEP, it can provide flexible standards for data protection in developing and developed countries. Bridging the gap between the economic level of developed and developing countries to promote the further formation of a wider range of multilateral cooperation and multilateral agreements. Similarly, the WTO, as the world's trade organisation, is working to establish a conflict-resolution, harmonised and coordinated e-commerce agreement. The aim is to reconcile the differences in digital governance between regions, mitigate conflicts in management policies, build a consensus on co-operative governance, and enhance the enforceability of cross-border governance of data and information.

6. Summary

Cross-border flow of data is the primary way of economic, cultural and news interconnection in the current world. While creating economic miracles and bringing convenient life to the public, it cannot avoid facing cyber threats of hacking, data leakage, malicious theft, invasion of privacy, and endangering national security. Therefore, secure cross-border data flow is a core issue for every country (region). Some domestic laws as well as regional rules (like RECP, DEPA, APEC Privacy Framework, GDPR) have already begun to practice how to promote the free flow of data while ensuring the security of data in their countries (regions). There are levels of scrutiny for personal information, trade secrets, and national secrets. However, there is no global regulatory legislation and rules in the area of cross-border data flows. Regionalised or inter-national governance is ultimately not a long-term solution. For example, the"long arm jurisdiction" by EU inevitably leads to judicial conflicts with other jurisdictions. Therefore, efficiently addressing the security risks of data flows requires a coordinated and consistent governance framework worldwide. The fundamental

differences in values and governance models between jurisdictions should be mitigated to reduce jurisdictional conflicts over the movement of data outside their borders.

References

[1] Jacques Bughin. The ascendancy of digital trade: A new world order? 2016 Retrieved from https://www.oecd.org/forum/oecdyearbook/ascendancy-digital-trade-new-world-order.htm.

Stren, Blan Partners. $1.3 BILLION FINE ON META: THE COMPLEXITIES OF CROSS-BORDER DATA TRANSFER IN A DIGITAL WORLD,

[3] Stren, Blan Partners. $1.3 BILLION FINE ON META: THE COMPLEXITIES OF CROSS-BORDER DATA TRANSFER IN A DIGITAL WORLD, 2023. Retrieved from https://strenandblan.com/2023/07/17/1-3-billion-fine-on-meta-the-complexities-of-cross-border-data-transfer-in-a-digital-world/.

[4] IBM Security, Cost of a Data Breach Report,2020. Retrieved from https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf.

[5] World Economic Forum. The Global Information Technology Report, 2016. Retrieved from https://www.weforum.org/reports/the-global-information-technology-report-2016/.

[6] Liyuan Sun, Hongyun Zhang, Chao Fang. Data security governance in the era of big data: status, challenges, and prospects. Data Science and Management, 2021,2: 41-44.

[7] Jingbo Dong. Security governance of cross-border data flows. Science&Technology Review, 2021,39: 9-17.

[8] IBM Security. Cost of a Data Breach Report, 2020. Retrieved from https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf.

[9] Anupam C. Data nationalism[J]. Emory Law Journal, 2015, 3: 678-739.

[10] Duo Zhang. Study on the Legal Regulation of Cross-border Data Flows. Social Science, 20181:116-119.

[11] Kangjia Liu. On the Regulation of Cross-Border Data Flows: Models, Challenges and Responses. Social Science, 2023 44(4):49-53.

[12] The Law of the People's Republic of China on the Preservation of State Secrets, Article 48.

[13] The Regulations on the Administration of the Credit Collection Industry, Article24.

[14] The Circular of the People's Bank of China on the Effective Protection of Personal Financial Information by Banking Institutions, Article 6.

[15] The Measures for the Administration of Population and Health Information, Article 10.

[16] The Regulations on the Administration of Maps, Article 34.

[17] Meili Wang, Yu Chen. A Study on the Mapping of China's Data Cross-Border Flow Rules with the CPTPP. International Trade Journal, 2022,20:20-29.

[18] Rui Wang. The Primary Content and Influence of GDPR. Financial and Accounting, 2018, 8:17-26.

[19] Jessica Shurson. Data protection and law enforcement access to digital evidence: resolving the reciprocal conflicts between EU and US law. International Journal of Law and Information Technology, 2020,28:167-184.

[20] Peter Swire. When Does GDPR Act as a Blocking Statute: The Relevance of a Lawful Basis for Transfer. Georgia Tech Scheller College of Business Research Paper, 2019:1-18.