LUMS | Centre for Chinese Legal Studies

Construction of Governance Scenario of Cross-Border Data Flow in the "Digital Silk Road"

Zhao Wanru[1]

[1] Institution of Cyberspace Governance, Wuhan University, Wuhan, China, 430000

Abstract: In order to facilitating cross-border data free-flow, satisfying the growing demand for data using, and accommodating the flourishing development of worldwide digital economy, this article aims to give a governance scenario of data flow in the “Belt and Road”. The author states the legal needs of relative countries by comparing the existing regulatory mechanisms of cross-border data free-flow in Europe and the United States, analyzes the differences in the operation of the existing data regulation mechanisms in the “Belt and Road” region, and proposes governance paths for the flow of personal and non-personal data across this region. Firstly, for cross-border flow of personal data, countries in this region should clarify the exemption criteria for localized storage and build an "adequacy protection" recognition system on this basis. Secondly, for the cross-border flow of non-personal data, countries in this region should jointly establish a hierarchical catalogue for the management of data in the region, set a minimum localization standard for data leaving the country and ensure the free flow of non-sensitive data to the maximum extent. Finally, countries in “the Belt and Road” region should abandon unilateralism in governance, strengthen consultation and deepen cooperation, discuss and share the "Belt and Road" framework for cross-border data flow, and promote the "Digital Silk Road. The "Digital Silk Road" should be built to facilitate the prosperity of the digital economy of countries along this region.

Key words: “Digital Silk Road”; Digital economy; Data Cross-border; Local storage of nationalized data; the “Belt and Road”

1. The significance of cross-border data flow governance in facilitating “Digital Silk Road” construction

The world is in the new explosion of industrial revolution. Data is as a factor of production in the digital era, data-based algorithms and arithmetic capabilities are redefining the status of a country's critical productivity development. Digital economy is progressively becoming an important contributor to global economic growth. In digital economy, the flow of data underpins virtually all types of globalization activities and is gradually becoming an essential factor in promoting national economic dynamism. Under the background, the “Digital Silk Road” is a combination of the development of the digital economy and "the Belt and Road". Initiative, it is an integral product of the globalization of the digital economy, aiming to build sustainable development economy based on digital technology. At present, most of countries along the "Belt and Road" are developing countries. They are still in the initial period of digital transformation with discrepancies degree of national Internet technology development. And the challenge of "digital divide" is still

obvious, which has created "digital isolation" with the global community. With the aim of enhancing the digitization of countries along the “Belt and Road”, accelerating digitization and releasing the potential of digital economy growth in the area, it is imperative to devise a digital governing system suitable for the extent of regional development and unition of the consensus of all countries, to advance the construction of the “Digital Silk Road”, and to cooperate in promoting a new model of digital globalization.

The recent global COVID19 epidemic accelerates the worldwide digital transformation, but also provides a historic opportunity for countries along the Belt and Road to bridge the digital divide and achieves economic prosperity. In order to grasping this unique historical opportunity, countries along the route should break down barriers to data flow and facilitate the free flow of data within the region under this strategic framework of the “Belt and Road”.

But diversity of countries' interests in data legislation due to their different levels of Internet development has further led to a trend of unilateralism in data governance in the “Belt and Road” region. It is not conducive to the mutual trust and integration of countries in the process of regulating cross-border data flows, increasing the compliance costs of enterprises in data flows. It also hinders the free flow of data in the region. To this end, it is crucial for the construction of the “Digital Silk Road” to build a governance framework for data cross-border flows, and help countries reach a consensus on governance and achieve a state of free flow of data within the region.

2. Main concerns of cross-border data flow governance in the “Belt and Road”

2.1. Lacking of data governance cooperation of relative countries

At present, countries along the "Belt and Road" mainly adopt unilateral regulation of data regulation, supplemented by some bilateral agreements, and have not established a coherent and unified legislative system. Main reasons are that, on one hand, countries are at different stages of Internet technology development, leading to divergent interests and different legislative policies. On the other hand, countries are belonged to multiple legal systems and sources, and the legal concepts, legal application techniques and legal expressions under different legal systems are diverse, so countries are unable to comprehend each other's legislative systems. Consequently, countries are unable to understand each other's legislative systems. This causes great obstruction for mutual understanding and application of the legal systems of the countries along the digital economy and trade routes. [1]

Besides this, lacking of institutional basis for mutual understanding leads to weak impetus for existing data cross-border mechanisms across countries. The ASEAN Data Management Framework (DMF)[2] and the ASEAN Model Contractual Clauses for Cross Border Data Flows (MCCs)[3] are main achievements for the “Belt and Road”. These are the China-ASEAN regional cooperation mechanism to design cross-border data flow. Nevertheless, the two ASEAN Model Contractual Clauses have not become a common rule adopted by countries along the “Belt and Road”, and international cooperation on the cross-border flow of personal data in the region is still limited to bilateral free trade agreements.

2.2. Personal data flows: unclarity of standards in intro-domain localization exemptions

The differences in the development of the data industry among countries along the “Belt and Road” have caused most of them to adopt a widespread model of data localization regulation in order to maintaining their own data security, with the exception of data that meets the requirements of the localization exemption, which may break data flow restrictions.

The currently accepted principles for exemptions include the principle of explicit consent of the data subject and the principle of adequacy decision. Firstly, data proprietary rights depend on the data proprietor and often reflect his or her property values and personal characteristics.[4] The values of the data must be separated from the relationship of proprietorship and the consent of the data subject must be obtained. Generally speaking, the principle of the explicit consent of data requires that data may infringe on personal, national security or public interest be prohibited from leaving the country without the explicit consent of the data subject. However, there is no specific express consent procedure specified in the data legislation of countries along the “Belt and Road”, and the relevant legislation only stops at the level of principle, which is not easily operable for implementation and affects the efficiency of data transfer.

Secondly, the principle of adequacy decision refers to a strategy for assessing the security conditions of data transfers with reference to the level of adequate data protection by third parties. For this purpose, it is required that only the receiving country provides the equivalent level of data protection when transferring data abroad. It requires that only if the data receiving countries provide the equivalent level of data protection for the flow of data abroad, data proprietor's express confirmation can be waived. Otherwise, the data subject is permitted to take the appropriate measures to interrupt the data flow process. While countries along the “Belt and Road” are active in adopting the principle of adequate protection as an exemption for data localization storage. In addition, the evaluation criteria of adequacy are not consistent among countries and the procedures for evaluating adequacy are unclear, which makes it inapplicable to specific cross-border situations and affects the efficiency of data flow in cross-border practice.[5]

2.3. Non-personal data: unclarity of intro-domain prohibition of data flow standards

In the process of data flow, in order to avoiding critical information related to national security from being illegally analyzed by decryption software and then exploiting data vulnerabilities to steal information to endanger national data security. Thus, most countries have adopted the principle of territory-based legislation for the localization of data related to national security and limiting the flow of such sensitive data to the territorial jurisdiction of the country.

At present, countries along the " Belt and Road" have developed the classification of territorial restrictions in following ways: Firstly, for general data, only intra-domain storage is required, with no restriction on accessing and processing location. Secondly, important data requires the localization of storage, but allows extra-domain access. Thirdly, critical data involving public security requires the storage, processing and accessing to absolute localization. By adopting the legislative model of hierarchical data transfer regulation, countries intend to build a secure and reliable foundation for data free-flow within the region. On the contrary, due to the differences in data legislation among countries within the region, the prohibition of data flow criteria is variant, and the arbitrary indiscrimination and unilateral prohibition of data flow criteria can also result in data trade barriers hindering the development of digital economy within the region.

Hence, in order to addressing the unreasonable obstacles that arise in the hierarchical regulation

of data and to form a relatively moderate model of secure data flow, various international organizations have engaged and developed diverse data embargo standards. The embargoed standards developed by international organizations, however, do not clearly indicate specific rules for their application, making it uncertain whether they can be adapted to the aims of each country's data storage, and harder to counteract the risks of data transfer and ultimately fail to compensate for the dilemma of different data legislation in each country. When constructing a viable embargo standard system, therefore, thoughts should be given to how to balance the relationship between data protection and free flow, to remedy the dilemma of differing national data legislation and achieve the free flow of data in a secure environment.

3. Current inter-regional experiences of cross-border data governance

3.1. EU cross-border data governance system

Determining the minimum standard of public interest identification based on balancing the claims of national interests and national public security. The EU, as a representative region for current legislation on cross-border data flows, published the *General Data Protection Regulation* (GDPR)[6] and the *Regulation on the Free Flow of Non-personal Data*[7] in 2016 and 2018, which adopt various strategies for personal data and non-personal data respectively. This new technology has already posed a challenge to European sovereignty and the implementation of the General Data Protection Regulation: how to determine who is the data controller? How to determine data flow out of the EU? Does European jurisdiction cover globalized cloud storage[8]?

3.1.1. Regulation of cross-border flow of personal data

Under GDPR, the EU classifies personal data flow situations as intra-EU flow and flow to third countries or international organizations, and sets out different levels of data protection standards for each situation. [9]

Within Europe area, data free-flow is the principle and restricted flow is the exception. Due to the high degree of integration in the EU, the GDPR is directly effective for EU members, and the synchronization of the development of the digital economy and the level of protection of personal privacy among countries, personal data can therefore generally be transferred freely between members. Meanwhile, GDPR allows member states to make specialized provisions on the content of certain articles based on legitimate policy objectives, without violating the principles of the GDPR.[10] In that case, the intra-domain data flow must also satisfy the particular provisions of the domestic law of the members. As GDPR extends the regulation of the receiving of personal data to third countries or international organization, however, even if the receiving party is an international organization within the EU, it should pass the EU's 'adequacy evaluate' [11].

For data flow outside the EU, the EU is based on the principle of "adequacy" with an exception for the principle of informed consent of the data subject. In general, the EU requires "adequate level of protection" for data receiving parties, which means the EU requires member states to restrict the transfer of personal data from their territory to outside the EU, unless the receiving party is certified by the EU as having a ‘adequate level of protection’.

Article 45(2) of the GDPR sets out detailed criteria for determining "adequacy": Firstly, the extent of the rule of law, the safeguarding of human rights and the legislative and administrative structure, the involvement of state authorities in the powers of data controllers in the territory, and

the rights and remedies guaranteed to the data subjects, in the data transferring countries. Secondly, a review of the relevant international commitments already undertaken by third countries or relevant international organizations. In addition, the EU provides for a system of occasional recertification, whereby third countries that are deemed not to be providing adequate protection shall notify each other, and member states shall take the appropriate measures to actively interrupt the flow of data to the region in the case of third countries that are considered to no longer satisfy the adequacy requirements[12].

Through this audit system, the EU ensures the effective implementation of the principle of "adequacy", avoids ineffective legislation due to lacking promotional mechanisms and helps to establish uniform standards for the cross-border transfer of personal data. Furthermore, in the absence of an adequate standard of protection or appropriate protective measures, personal data may be transferred abroad outside the scope of the "adequacy of protection" principle if the data subject consents to the transfer to a third country or a national organization after having been expressly informed that the transfer may pose a risk to him or her due to the absence of an adequate standard of protection and appropriate protective measures, as provided for in Article 49 of the GDPR. [13]

3.1.2. Regulation of cross-border flow of non-personal data

Following the publication of the Regulation on the Free Flow of Non-personal Data, in May 2019, the EU published Guidance on the Regulation on a Framework for the Free Flow of Non-personal Data in the European Union. In accordance with this, the EU aims to achieve the free flow of non-personal data within member states to provide incentives for industries to develop self-regulatory codes of conduct in relation to data transfers, prohibit member states from regulating the localization requirements for non-personal data, and make exceptions only on grounds of public security consistent with the principle of proportionality.[14]

In February 2020, the European Union published a European Strategy for Data which explicitly exempts the free flow of data from jeopardizing public safety, order and other legitimate public policy objectives. With regards to the movement of non-personal data, the EU currently only provides for rules regime where the movement within the territory is based on the principle of free flow, with the exception of restrictions in the public interest, and does not address the situation of the movement of non-personal data outside the territory.

The EU's territorial based data legislation depends on a high degree of integration between EU countries. Comparing to more fragmented cooperation of countries along the “Belt and Road”, the crucial factors of the EU to achieve a unified data governance within its territory are as followed: Firstly, the EU, as the most integrated international intergovernmental organization, has legislation that is directly applied to its member states, making it a more convenient to form a unified data legislation framework in the region. The "Belt and Road" economic belt spans a wide area and covers countries across Eurasia, which does not have the prerequisites for integrated legislation and cannot form an integrated data regulation framework； Secondly, the majority of EU member states are developed countries, and the level of Internet development is more synchronized among countries, which makes it simpler to reach a consensus on data legislation because of their relatively close interests. In contrast, the different stages of technological development of the Internet in countries along the “Belt and Road” lead to various national interests and demands, making it complicated to reach a consensus on legislation governing cross-border data flows that takes into account the interests of all countries. Last but not least, the European Continent has a shared tradition

of civil law legislation, and the legal systems of different countries are closer to each other, so it is more likely that uniform data legislation will be accepted and applied by all countries in the region. On the opposite side, the different historical and cultural backgrounds of the countries along "the Belt and Road" have led to the selection of legislation from different sources and legal systems, and the different legislative approaches of countries with diverse legal systems have made it incomprehensible for countries to understand each other's data legislation, increasing the cost of data flow within the territory.

As a consequence, the cross-border regulation of data in the “Belt and Road” refer to the EU's specific regulation model of data classification and sub-circumstances, setting different levels of restriction standards for different types of data in different flow situations. For the extraterritorial flow of personal data, reference can also be made to the EU's terrestrially-based "adequacy" principle, supplemented by an occasional audit system, to build a secure extraterritorial flow mechanism for personal data. For non-personal data, an intro-territorial regulation model based on the principle of free flow with public interest restrictions as an exception can be set.

3.2. US cross-border data governance system

The US, as a giant country in the internet industry, has mainly used its absolute leadership in the digital economy and trade to aggressively pursue cross-border data-free flows and solidify its dominant position in the internet industry sector. It adopts a completely different regulatory path than the EU in terms of cross-border data flow. [15]

3.2.1. Regulation of cross-border flow of personal data

The US regulatory path for personal data flows is based on the principle of minimizing data hold-ups and maximizing the free flow of data. Unlike the EU's uniform legislation, which is a preventive model of ex ante review, the US pursues an ex post regulatory path of penalties based on the principle of accountability. This legislative value proposition is reflected not only in the US domestic data regulation, but also in the US-lead regional economic cooperation agreements for data regulation.

The US regulatory model relies primarily on industry self-regulation, supplemented by government regulation. In terms of data governance, the US domestic data regulatory framework is constructed on the basis of the Privacy Shield Principles set by the Federal Trade Commission, on which the industry alliances and privacy certification companies then set specific corporate privacy qualification standards.[16] Guaranteeing the free flow of data when making the data controller or data processor responsible for the security of the data in a lawful and reasonable manner, otherwise the regulator will be held accountable. There are two levels of privacy protection standards within the US industry: the recommended guidelines published by the Online Privacy Alliances (OPA) and two mandatory binding privacy protection schemes developed by TRUSTe and BBB Online, two major US privacy certification companies. The guidelines published by the Online Privacy Alliance focus primarily on protecting data subjects' right to know about their data, and the Privacy Certification Enterprise Scheme's privacy protection scheme is a corporate privacy protection certification standard based on the OPA's constructive guidelines and incorporating the privacy protection principles published by the Federal Trade Commission. As a result, in order to qualifying for personal data processing, internet companies in the US must then meet the protection standards by certification body and pass the examination.

The US-lead regulatory path for international data flows advocates the elimination of localization policies and the introduction of lower data security protection requirements, essentially creates an enabling policy environment for data flows to the US. The 2012 US-lead system of cross-border privacy rules is an operational regime of specific rules for cross-border data flow in Asia-Pacific region developed under the APEC privacy framework.[17] Therefore, the CBPR system is government-supported initiative based on voluntary principles to provide companies with data privacy protection certification system that meets the recognized standards of APEC member countries.

3.2.2. Regulation of cross-border flow of non-personal data

For non-personal data, the US does not regulate the cross-border flow of non-personal data in specific regulations, rather the criteria for restricting exit are scattered throughout other relevant legislation. For illustration, the United States restricts the export of controlled items, commodities, technology, software or other types of unclassified controlled information to foreign nationals or entities without government approval under the Export Administration Regulations and the International Traffic in Arms Regulation.[18] Based on the above regulations, it can be concluded that, in other countries, for confidential data that may be related to national security and public privacy, prior approval must be obtained from the government before export, otherwise no cross-border flow is allowed. It can be seen that for non-personal data, the US has a complete freedom of flow for non-confidential commercial data, while for critical and sensitive data such as national security, the US also adopts pre-departure review mechanism.

3.3. Similarities and differences between US-lead CBPR system and EU-lead GDPR system

The US has been actively pursuing a CBPR-lead system of cross-border data regulation within the framework of APEC cooperation, and has introduced the CBPR system into several bilateral free trade agreements that include the US as a reference to enhance the compatibility of personal information protection mechanisms. In addition, the US is seeking to expand the CBPR beyond the APEC region to form a regulatory regime for cross-border data flows that can compete with GDPR.

In comparison to the top-down regulatory system of the EU GDPR, the CBPR places greater emphasis on self-regulation based on voluntary principles, resulting in a more mobile and flexible enforcement mechanism than the GDPR. It requires participants to have at least one APEC-accredited accountability agent that is responsible for providing third-party certification to companies. In addition to requiring member states to have independent data protection authorities, the GDPR also establishes the EU Data Protection Board to be responsible for the uniform implementation of the GDPR within member states. Compared to the implementation mechanism, which must be consistent among EU member states, the CBPR delegates governance powers by authorizing independent audit qualifications to each participant, increasing the efficiency of the regulation. As a result, the CBPR establishes only a bottom-line standard, whereas the GDPR provides for a detailed review of adequacy. [19]

The interconnection between the US-lead data cross-border system and the EU-lead GDPR system is mainly reflected in the dual certification of the EU Binding Corporate Rules (BCR) and the CBPR. For example, in 2012, the EU and APEC set up a joint working group to attempt to establish a harmonies agreement on both the CBPR and GDPR privacy protection standards and adequacy certification mechanisms for data processors to facilitate further free flow of data across

borders between two systems. Though specific implementation standards are not yet in place. Despite the vast differences in regulatory paths between the European and American systems, both include data processors in the scope of regulation. This attempted convergence reduces the cost of compliance for data processors in cross-border data flows by using the data processor, the object of uniform regulation, to develop a mutually acceptable double standard, which fundamentally contributes to the efficiency of the further free flow of data. [20]

The US data strategy is based on its overwhelming superiority in the digital industry and trade, using its advantages to enforce the value of "data freedom" legislation within global trade and economic agreements in order to protect the interests of its own internet giants. United States has gradually established a system of cross-border data systems based on the value of the free flow of data through a series of trade agreements, incorporating US regulatory claims into binding economic and trade agreements and thereby integrating them into the global trade and economic rules system.

On the contrary, the “Belt and Road”, as a collaborative development initiative of mutual friendship and assistance, does not have the absolute advantage of exporting its own legislative values to the countries along the route. On the other hand, China always upholds the development concept of joint progress and common prosperity, and insists on joint governance for the construction of cross-border data flows in the “Digital Silk Road”, balancing the interests of various countries and rejecting the governance approach of data hegemony. Thus, for the construction of the data governance system in the “Digital Silk Road”, reference can be made to the US industry self-regulatory review model for personal data flows as a supplementary rule for data governance, to improve the level of data protection in the industry, promote the level of data protection in the countries in the region to approach the existing European and American standards, and lay the institutional foundation for data processing in a wider scope for enterprises in the region in the future.

4. Construction of cross-border data governance system in "the Belt and Road" region

The real necessities of social development foster the prosperity of digital trade, and the development of digital trade drives the emergence and evolution of global digital value chains. Under the background of economic globalization, whether data can flow freely across borders directly affects the business efficiency of the relevant subjects in digital value chains. Therefore, in the process of jointly pushing forward the construction of the “Digital Silk Road”, it is essential for countries in the region to refer. It is also necessary for these countries to jointly build a scientific and reasonable governance system for cross-border data flow in response to different specific transport scenarios, to overcome the current dilemma of data flow compliance due to the lack of regulation, and form a governance mechanism for cross-border data flow sharing along the “Belt and Road”.

4.1. Personal data flow: clarifying exemption criteria and building a recognition mechanism

For the " Belt and Road" cross-border data flow regulation, the protection of personal privacy is the consensus of national legislation. However, current standards and procedures for localized exemptions are unclear, resulting in a lack of universal procedures for the implementation of standards and procedures for the protection of personal privacy among countries. Accordingly, this article argues that it should be learned from the characteristics of the US "industry self-regulation" model and the EU data subject express consent procedure to form a data regulation system that

taking into account the regional background of the “Belt and Road”, enhancing the awareness of personal data privacy protection in countries along the route, and promoting the convergence and mutual recognition of internal standards with international standards. The data governance dilemma mentioned above regards the unclear process for determining exemptions for local storage of personal that data can be resolved by making corrections to the lacking parts of the current exemption criteria.

4.1.1. Clarifying data subject's express consent determination process

As the level of internet development varies among countries in the region, some countries have difficulties in reaching adequate standards of protection of personal privacy at the level of data legislation due to the backwardness of legislative technology. Under the background, with attempt to remove barriers to data crossing borders, compensate for the blockage of data flows due to insufficient legislation and realize the genuine expectations of data proprietors with regard to data transfers, countries can construct relevant identification procedures by means of ex-ante disclosure of processing procedures by data processors and ex-post online fixation of evidence of data subjects' confirmation.

The procedures, as described above, are as follows: Firstly, the data processor should make clear to the data subject the purpose, scope, type, quantity, social and economic value, sensitivity and technical processing of the data exiting the country before collecting the data, and warning labels for sensitive information about the data subject. Secondly, the data subject shall expressly consent to the parts explicitly stated by the data processor, and be presumed not to consent to the parts that increase the risk burden on the data subject if the data subject does not expressly consent to them. Thirdly, the data processor shall obtain and be back up in a reasonable manner the data subject's confirmation to the content and temporal information of the flow in respect of the data subject's express consent in various forms.

4.1.2. Refining the criteria for evaluating adequacy protection

In order to reducing the security risks of personal data flow in the region, improving the efficiency of data flow, and countering the flow risks caused by the insufficient level of protection during data flow, it is essential for countries to refine the adequacy protection evaluation criteria and build evaluation system to improve the level of data protection in the countries.

As is regarded, the specific procedures are as follows: Firstly, the criteria for assessing the adequacy of the protection of personal data privacy in the data receiving countries are defined, mainly by reference to the EU legislation on the assessment of privacy protection in the data receiving countries, based on the general and sectional data protection provisions in force in the third countries, as well as the professional rules and security measures implemented in the country, the level of law rules, human rights protection, the effective functioning of independent regulatory agencies, data technology development in the receiving countries and the international unilateral or multilateral agreements to which they are party. Secondly, constructing intra-regional sufficient protective evaluation system. On one hand, organizing professional groups to evaluate security levels of data flow environment in relative countries. One the other hand, promoting industry self-regulation, founding cyber-tech industry associations by individual corporations, establishing universal standards of privacy protection, to felicitate protection levels of intra-regional cyber-tech corporations. Last, it is significant to promote mutual recognition of the “Belt and Road” data

protection system with current systems depending on influence within industry, and decrease the compliance costs of relative corporations.

4.2. Non-personal data flow: establishing a hierarchical and classified catalogue of regional data management

As overall data technology development level of the countries along the “Belt and Road” is relatively backward. If the data classification system under the US industry self-regulation model is applied, it will not only fail to achieve the purpose of data governance, but may also cause the unilateralism of data protection in the region due to the unrestricted data protectionist legislation of each country, which will hinder the development of the digital economy along the “Belt and Road”. If we stick to the strict restriction path of the EU model, it is not conducive to balance the conflicting data interests of countries and not practicable. In current situation of multiple values and conflicting interests in intra-regional legislation, it is more advisable for relative countries to abandon the mentality of competition and confrontation, reduce the requirements for localized data storage in the region on the premise of safeguarding the data security of each country, and explore the formation of data flow restriction rules that take into account the actual situation of each country along the route. As a result, for the situation of cross-border flow of non-personal data, the existing legislative and regulatory principles in Europe and the United States can be absorbed, and a model of free flow as the principle, with the prohibition of data transfer involving national security and public interest as the exception, can be built legislation on the regulatory path of non-personal data flow.

First of all, it should be clarified the standards of data prohibition in the territory and promoted the establishment of cross-border data security classification. Countries along the "Belt and Road" have diverse levels of Internet development and different domestic economic and social backgrounds, resulting in diverse interests in data legislation. The clarification of the prohibition of flow criteria is conducive to addressing the artificial barriers for cross-border flows resulting from the plurality of legislative systems. Among the main elements are risk assessment before data cross-borders and the establishment of a hierarchical and classified catalogue of data. National security and public order are currently recognized as legitimate data control grounds under the international data governance path, whether under the General Agreement on Trade in Services (GATS) and the Agreement on Technical Barriers to Trade (TBT) or the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP), which upholds the National Security Exceptional principle, means that countries may not accept or request information from others that is contrary to their national security interests. In Addition, "legitimate public policy objectives" has also been identified as an additional justification for exceptions to the free flow of data. The control of "data entry" in a country is basically for reasons of national security, cultural security, as well as national identity and ideology.[21] Thus, in the construction of the “Belt and Road” data classification catalogue, it is possible to draw on the experience of other multilateral rules that provide for the classification and protection of data related to national security and public interest. Based on this, it is also possible to count the content of data transfers from countries along the route through technical means, and set up a catalogue of data classification standards based on data analysis depending on the economy, laws, culture, religion and beliefs of each country, for reference in data transfers within the region.

Secondly, it is important to unify the standards of reasonable data flow restrictions in the region. However, the data flow restriction model set by countries in the “Belt and Road” region is conducive

to the construction of a secure data flow environment. On the other hand, lacking of unified regulation may lead to unrestricted expansion of the scope of restrictions through unilateral legislation, which may lead to barriers to the free flow of data and defeat the purpose of governance. Therefore, it is imperative to form industry-level data flow restriction standards that are compatible with data security protection and risk prevention in conjunction with the above-mentioned data classification catalogue, and to build a unified and applicable restriction system that balances the contradiction between local data storage and security ownership protection.

Lastly, the construction of a data security administration framework. Once the data has been classified and managed according to the security classification catalogue and rationalization criteria, it is necessary to establish a corresponding monitoring platform to monitor the data flow in time. As a result, firstly, an intra-domain regulatory information public platform will be set up to provide real-time updates on data legislation within each country. Secondly, risk assessment of data transfers and tracking of their use will be carried out according to the interests of each country. And thirdly, data governance experiences will be shared on a regular basis to pull the level of data governance within the domain and increase the speed of development of the data economy.

4.3. Facilitating the cooperation and construction of a common governance framework for cross-border data free-flow among countries along “the Belt and Road”

The development of the digital economy cannot be separated from the free flow of data in the region, and the prerequisite for the free flow of data is a well-established framework for data governance in the region. To advance the formation of a governance framework for cross-border data flows in the “Belt and Road” region, the participation of countries along the route is essential. Through the process of building the “Digital Silk Road”, we shall explore international data governance experience to coordinate the diverse interests of countries along the route and jointly develop rules for cross-border data flows that accommodate the development of the digital economy in the region. Countries along the “Belt and Road” should focus on the existing rule framework and dialogue, to bring into full effect the existing multi-bilateral trade agreements, strengthen consultations on the regulation of cross-border data flows in digital trade agreements, deepen international cooperation in the field of data flows among countries, and gradually bridge the gaps in the governance of cross-border data flows among countries. With a view to reaching a consensus on inter-regional collaboration on data governance for common development, to help build a connected "Digital Silk Road", jointly promote the development of the digital economy in "The Belt and Road" region, and build a further innovative regional cooperation agreement that is more accessible and tolerant.

5. Conclusions

As a fundamental strategic resource and an essential productivity for today's digital trade, data is a major driving force in fostering global economic development and has become central to the future development of national economic strategies in all countries. The "Digital Silk Road" is a new path for regional digital economy development proposed by China on the basis of the “Belt and Road” economic development initiative. In general, the current unilateralism in data legislation and the lack of a unified data cooperation mechanism in the “Belt and Road” region have led to unclear data governance standards and a jurisdictional vacuum. On the basis of advanced experiences from existing data governance paths in other regions, we should take the enhancement of the digital

economic community of destiny along the route as the core, uphold the attitude of seeking common ground while preserving differences, strive to overcome the barriers to data flow caused by the existing differentiated data regulation paths, form a unified data governance mechanism led by China, and lead countries to jointly promote the construction of the "Digital Silk Road".

Reference:

[1] Wang L. The Connection, Measurement and International Governance of Digital Trade Barriers [2021] 37(11) International Economics and Trade Research 85-100

[2] The ASEAN Data Management Framework [2021] OJ 1 241/03

[3] The ASEAN Model Contractual Clauses for Cross Border Data Flows (MCCs) [2021] OJ 2 32/47

[4] Qi P. Construction of the Governance Scenario of Cross-Border Data flow and Sharing in the "Belt and Road" Digital Economy [2022] 22(2) Journal of Beijing University of Technology (Social Sciences Edition)

[5] Lin J. & Tian C. On Regulation of Cross-border Flow of Personal Financial Data [2021] 38(06) Journal of Shanghai University (Social Sciences Edition) 95-107

[6] General Data Protection Regulation [2016] OJ 2 32/47

[7] Regulation on the Free Flow of Non-personal Data [2018] OJ 2 45/2

[8] Krinjar V. EU Data Protection Reform: Challenges for Cloud Computing [2016] 12(22) Croatian Yearbook of European Law&Policy 171-206

[9] Newman A. Building Transnational Civil Liberties: Trans-governmental Entrepreneurs and the European Data Privacy Directive [2008] 62(1) International Organization 103—130

[10] Zhang D. Research on Legal Regulation of Cross-border Data Flow (1st edn, University of International Business and Economics 2018) 166

[11] Fang F. & Zhang L. Governance Personenbezogener Daten der EU: Entwicklung, Dilemma und DenkanstoBe [2021] 36(04) Deutschland-Studien 49-66+157-158

[12] General Data Protection Regulation [2016] OJ 2 32/47

[13] Newman Abraham Innovating European Data Privacy Regulation: Unintended Pathways to Experimentalist Governance [2010]

[14] Kuner C. Transborder data flows and data privacy law [M] (2nd Oxford: Oxford University Press 2013) 31

[15] Chwartz Paul & J. R. Reidenberg Data Privacy Law: A Study of United States Data Protection [1997] Government Information Quakerly 14.2

[16] Li Y. Regulation Paht and China’s Choice on Global Cross-Border Data [Oct.2019] 0117(5) Presentday Law Science

[17] Li M. The Game and Cooperation on the Cross-border Data Flows Rulemaking between the US, Japan and the EU [Oct.2019] 02(5) Intertrade 88

[18] Nigel Cory Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? (Nigel Cory's website, 1 May 2017) <https: / /itif.org /publications /2017 /05 /01 /cross - border - data - flows - where - are - barriers - and - what - do - they - cost> accessed 13 February 2022

[19] Jia K. Conflict and Cooperation: Evolvement of Trans-Border Data Flows between US and EU [2017] 33(5) Journal of Shantou University 57-61

[20] Yan T. & Fan Z. The Governance Paradigm of Cross-border Data Flow between the US and

Europe and the Way Forward for China [2021] (06) Journal of International Relations 76-96+155
[21] Gong W. Information Sovereignty Reviewed [2005] 14(1) Intercultural Communication Studies 119-135