ISSN: 2710-0170

The Regulation of RCEP Data Cross-border Flows and China's Strategies in the Context of Digital Trade

Ziyi Liu [1], Ke Zhang [1], Jinqiu Jiang [1], Changqing Li [2] and Ye Ju [1,*]

[1] Faculty of Law, College of Applied Arts and Science, Beijing Union University, Beijing, China;

[2]Senior Partner, Long An Law Firm, Beijing, China;

*Corresponding Author: juye@buu.edu.cn.

Abstract

The RCEP regulation of cross-border data flow reflects the regulatory theory of "limited openness and prudent supervision", but in the balance between data localization and free flow, the ambiguity and binding nature of the exception clause lead to conflict in its application, and the adoption of the "Kaldor Hicks efficiency" standard to construct the institutional framework may improve the current dilemma. The adoption of the "Kaldor Hicks efficiency" standard to construct the institutional framework may improve the current dilemma. At present, the data protection legal system among RCEP member countries is fragmented, which is manifested in the diversity of legislative modes and regulatory priorities but has become a trend of convergence. The RCEP data cross-border flow regulatory system has conflicts in jurisdiction, legal application, law enforcement, etc., so it should optimize the path of synergy among legislation, judiciary and law enforcement; strengthen the interaction between the framework agreement and domestic laws; promote the deepening of cooperation and the construction of mutual trust; and promote the innovation and capacity building of the mechanism. Innovation and Capacity Building. In the RCEP cross-border data flow law, China should carry out multi-dimensional innovation of "system-mechanism-technology", form a new paradigm of differentiated regulation, build a multi-level collaborative governance framework with vertical and horizontal coordination and internal and external linkage, create a new model of cross-border secure data flow, and establish a dynamic technical protection system.

Keywords

Digital Trade; RCEP; Cross-border Data Flows; Conflict of Laws; Collaborative Governance Mechanisms.

1. Problem Formulation

With the booming development of digital technologies such as the Internet and blockchain, and the accelerated integration of digital and traditional industries, digital trade has become a new growth engine for international trade. The Regional Comprehensive Economic Partnership (RCEP), signed by 15 Asia-Pacific countries including ASEAN's 10 member states, China, Japan, Korea, Australia and New Zealand, represents the largest free trade agreement in the Asia-Pacific region. Based on the difference in the level of economic development, developed countries in the member states have invested much more than developing countries in the construction of data legal systems, such as China, Japan and Korea, may prioritize legal regulations concerning data protection, privacy rights, cross-border data flow security rather than focusing solely on promoting data circulation to enhance national competitiveness.

Diverse legal traditions and cultural backgrounds, as well as differences in countries' international status and interests, interact with each other to form the heterogeneity of the data

ISSN: 2710-0170

legal systems of member countries. The RCEP has special exception clauses to balance the flow of data and data security, and security exceptions to a large extent give member countries a certain amount of jurisdiction over data, but the scope of application of the exception clauses and the standards are still open to question, and there is uncertainty in application. With the intensification of the game between data security and commercial interests in member states and the intensification of the contradiction between data localization and free flow, the lack of a regional data governance synergy mechanism is becoming more and more prominent. How to build unified data rules to promote the free flow of data while ensuring data security, and how to balance the interests of member states to promote RCEP data governance from conflict to synergy, have become urgent issues. These issues not only concern the development of RCEP but also play a key role in the governance of global digital trade.

2. Legal definition of the core concepts of "data", "cross-border data flows" and "data sovereignty"

2.1. Legal attributes of "data": paradigm shift from object to quasi-subject

In traditional legal systems and concepts, "data" refers to any record of information by electronic or other means. Data, as a carrier of information, lacks the independence and specificity of objects in civil law and cannot exist independently of its technical environment. Data itself does not directly constitute property, and its property attributes mainly depend on its application scenarios and the way of value realization, which is often regarded as the object of property rights.

With the continuous development of the digital economy and the emergence of tools such as big data and artificial intelligence, the collection, processing, analysis, and use of data have been provided with strong technical support and safeguards, thus enabling the value of data to be fully exploited. The existence of rights and interests such as ownership, use, and income of data is gradually recognized and protected by law, and in the process of transaction, data is regarded as a valuable asset to be bought and sold, and the processor shall bear the corresponding legal responsibility in the process of collection, processing, storage, use, and transaction of data, and the complexity of the rights and interests network formed in the process grants the data a certain degree of The complexity of the network of rights and interests formed in this process has given data a certain degree of autonomy, thus making data, to a certain extent, exceed the scope of the traditional object of property rights and have a status similar to that of a legal subject.

In the future, with the rapid development of science and technology and the digital economy and the continuous improvement of the legal system, data will become an important factor of production and asset class, whose value will be further explored and exploited, whose quasi-subject status of legal attributes will be further clarified and made clear, and whose autonomy will be further expanded, even with the ability to make decisions and act on its own. There is a legal need to establish a more perfect regulation and protection mechanism so that data will assume more responsibility.

2.2. The Legal Connotation of "Cross-border Data Flows": A Game of Rights and Interests Beyond Geography

The understanding of cross-border data flows can be defined in two dimensions: first, the transmission, processing, and storage of data between different countries; and second, the ability of data to be accessed and used by entities in other countries, even if the data itself does not cross national borders. As a result, cross-border data flow can be summarized as the process of data transmission, processing, and storage between different subject entities and the resulting distribution of rights and interests and risk management activities. Cross-border data

ISSN: 2710-0170

flows are subject to the legal jurisdiction and regulation of multiple countries and territories and involve various legal areas, including data protection, privacy, national security, commercial interests, etc. The complexity of cross-border data flows increases as the intersection and conflict of these areas are often unavoidable. With the development of globalization and the acceleration of digital transformation, cross-border data flow is not only based on the territorial jurisdiction in the traditional legal system but also on the flow of data in geographic and physical space at the technological level, which is an important area for countries to transcend the territorial rights and interests of the game. Data has non-exclusivity; cross-border data flow allows a country to cross the traditional national boundaries to obtain data outside the country, contradicting the requirements of data localization, and is very likely to involve the leakage of core data, thus infringing on the country's data sovereignty and triggering national security risks. Based on the multidimensional and dynamic nature of cross-border data flows, risk management and control of cross-border data flows are particularly important in order to prevent the above problems of breaking through economic, cultural, and even legal boundaries.

In the context of the digital economy era, cross-border data flow has become a link connecting the global economy. Based on the above analysis, how to define the jurisdiction of data in the virtual space and how to balance the relationship between privacy, data sovereignty, and national security in the process of promoting cross-border data flow so as to realize the standardization, liberalization, and securing of the global data flow has become a current need to rethink and urgently need to It has become an issue that needs to be rethought and urgently resolved.

2.3. Jurisprudence of “data sovereignty”: digital reconstruction of the concept of sovereignty

In the traditional concept, sovereignty means that a state enjoys supreme jurisdiction over everything within its territory. With the acceleration of the global digitalization process, the emergence of new factors of production and strategic resources, the emergence of data as a core element of national competitiveness, the increasing frequency of cross-border data flows, and the growing severity of new types of security threats such as data theft and cyberattacks, the application of the traditional concept of sovereignty in the field of data is facing unprecedented challenges. Expanding the scope of traditional sovereignty from physical space to cyberspace and data, and digitally reconstructing the concept of traditional sovereignty to safeguard national security and promote the development of the digital economy, have become the mainstream trend nowadays, and the concept of data sovereignty has come into being. Data sovereignty is summarized as the highest authority a country enjoys over the data infrastructure, data resources, data subjects, and their data behaviors within its own territory based on national sovereignty , and it is the sum of a country's rights and capabilities to safeguard its national interests and citizens' interests in digital space and participate in global data governance, which is of great significance in safeguarding the interests of the development of data resources and in maintaining the safety of the people and the security of the country in cyberspace. It is of great significance in safeguarding the interests of data resources development and maintaining people's security and national security in cyberspace and has now become a new type of resource for countries to compete in cyberspace.

However, many challenges remain in the process of digitally reconfiguring the concept of sovereignty. How to balance the flow and sharing of global cross-border data while upholding data sovereignty has become an important challenge for the world. If data sovereignty is overemphasized, it may lead to the formation of data silos, thus hindering the development of the digital economy; if data flows are left completely unchecked, it may threaten national security and the interests of citizens, thus undermining national sovereignty. Therefore, a

ISSN: 2710-0170

country's adoption of differentiated sovereignty strategies for different types and sensitivities of data is an effective move to balance national and global interests. For core data involving national security, strict sovereignty control should be adopted to safeguard the core national interests and prevent external forces from using the data to carry out infiltration and sabotage activities, thus guaranteeing national security; for ordinary commercial data, a more open strategy should be adopted so as to reserve the corresponding space for the development of the global data economy. The above can be summarized as the concept of resilient data sovereignty, the proposal and practice of which are of great significance in adapting to the needs of the digital era, safeguarding national security, and promoting global data cooperation and governance. And it is the sum of a country's rights and capabilities to safeguard its national interests and citizens' interests in digital space and participate in global data governance, which is of great significance in safeguarding the interests of the development of data resources and in maintaining the safety of the people and the security of the country in cyberspace. It is of great significance in safeguarding the interests of data resources development and maintaining people's security and national security in cyberspace and has now become a new type of resource for countries to compete in cyberspace.

However, many challenges remain in the process of digitally reconfiguring the concept of sovereignty. How to balance the flow and sharing of global cross-border data while upholding data sovereignty has become an important challenge for the world. If data sovereignty is overemphasized, it may lead to the formation of data silos, thus hindering the development of the digital economy; if data flows are left completely unchecked, it may threaten national security and the interests of citizens, thus undermining national sovereignty. Therefore, a country's adoption of differentiated sovereignty strategies for different types and sensitivities of data is an effective move to balance national and global interests. For core data involving national security, strict sovereignty control should be adopted to safeguard the core national interests and prevent external forces from using the data to carry out infiltration and sabotage activities, thus guaranteeing national security; for ordinary commercial data, a more open strategy should be adopted so as to reserve the corresponding space for the development of the global data economy. The above can be summarized as the concept of resilient data sovereignty, the proposal and practice of which are of great significance in adapting to the needs of the digital era, safeguarding national security, and promoting global data cooperation and governance.

3. Current Status and Comparison of Legal Regulation of Cross-border Data Flows in RCEP Member Countries

3.1. Diversity and Convergence of Legislative Models for Cross-Border Data Flows in RCEP Member Countries

RCEP member countries differ in their specific legislation on cross-border flow of data, with some adopting a more stringent censorship regime while others are relatively open. In terms of the legislative hierarchy, the regulatory models of member countries can be broadly classified into three categories: comprehensive, specialized, and decentralized legislation. Despite the differences in national legislative models, there has been a convergence of data classification and management, security assessment mechanisms, and cross-border flow conditions, reflecting the convergence of regional data governance rules.

ISSN: 2710-0170

Table 1 Legislation related to cross-border data flows in RCEP member countries

Types of legislative models	On behalf of the State	key feature	regulatory focus	Typical legislation
Comprehensive legislative type	China, Japanese	Enactment of a unified data protection law to systematically regulate the cross-border flow of data	Data security and privacy protection go hand in hand	Personal Information Protection Law (China), Personal Information Protection Law (Japan)
Specialised legislative type	Korea, Singapore	Specialised legislation for specific areas of data	Focus on personal data protection	Personal Information Protection Act (Korea), Personal Data Protection Act (Singapore)
Decentralised legislation type	Selected ASEAN countries	Adoption of multiple laws to regulate different types of data separately	Focus on industry regulation and data security	Cybersecurity Law (Viet Nam), Data Privacy Law (Philippines)

3.2. Differences and Commonalities in the Regulatory Priorities of Cross-Border Data Flows in RCEP Member Countries

RCEP member countries have demonstrated "layered control" in the regulation of cross-border data flows, which is mainly reflected in the balance between the free flow of data and exception clauses, data classification and protection, and prudential regulation of industries. The "layered control" regulatory model not only reflects support for the free flow of data, but also fully takes into account and safeguards data security and national interests, and demonstrates the combination of specific rules and diversified practices of member countries.

Table 2 Comparison of regulatory differences and commonalities in cross-border data flows among RCEP member countries

Regulatory dimension	Developed economies (Japan/Singapore/Korea)	Developing economies (China/Indonesia/Vietnam)	commonality
Regulatory focus	Free flow of data, facilitating digital trade	Data sovereignty, security control	Data Security Assurance
Data localisation	Localisation required only for specific industries (e.g. finance)	General requirement for local storage of important data	Classification and Hierarchy Management
cross-border transmission	Adoption of a sufficiency determination mechanism with relatively simplified procedures	Requirement of security assessment and strict approval process	Establishment of a review mechanism
Protection of personal information	Comprehensive legislative protection	Progressive improvement of specialised legislation and enhanced protection	Enhanced protection

ISSN: 2710-0170

industry regulation	Industry self-regulation is the main focus	Government regulation as the mainstay, multi-level regulatory system	Multi-level regulatory system
Enforcement efforts	medium	severity	Penalties are clear
International cooperation	Active participation in international rule-making	Prioritising domestic regulatory frameworks and recognising the need for international cooperation	Recognition of the importance of international cooperation

The legislative models and regulatory priorities of cross-border data flow regulation in RCEP member countries are characterized by diversity and complexity, reflecting the different considerations of member countries in terms of data security and industry regulation. At the same time, it also provides opportunities and challenges for member states to cooperate and coordinate the regulation of cross-border data flow. With the advancement of the digital era, RCEP member states need to further strengthen communication and cooperation, and promote the legal regulation of cross-border data flows towards coordination and unification.

4. RCEP Regulation of Cross-Border Data Flows Examination and Jurisprudential Analysis

4.1. RCEP Cross-Border Data Flow Regulation Examination

Chapter XII of the RCEP on electronic commerce adopts a three-tier structure of "General Provisions—Specific Norms—Exceptional Reservations," in which the norms on cross-border data flows reflect the regulatory rationale of "limited openness and prudential regulation".

Article 14 of the chapter clearly stipulates the basic principles of cross-border data flow, adopting a "negative list" model with the promotion of free flow of data as the benchmark, supplemented by necessary restrictive measures. In terms of normative effect, the cross-border data flow rules established by RCEP adopt the institutional design of "soft law first". By excluding the data flow rules from the dispute settlement mechanism, member states are given more policy space in the process of implementing the rules.

Although the mandatory binding force of the rules has been weakened, the soft law untied with a large elasticity space leaves room to reduce the touching of the sensitive nerve of the state in defending its sovereignty and its valued rights and powers, which is of practical significance in balancing data sovereignty and trade facilitation. In addition, RCEP takes into account the differences in the development of member countries, which is conducive to achieving the dual goals of cross-border data flow and the development of digital trade, reducing the conflict between the domestic laws of member countries and achieving mutual compatibility.

With regard to the balance between data localisation and free flow, which has attracted much attention, RCEP basically follows the rule structure of "limited commitments + flexible exceptions." According to the provisions of Article 15(3)(b) and (c) of Chapter XII, RCEP adopts a "double standard of review" in the setting of restrictive measures on cross-border data flows. First, the restrictive measures must be premised on the achievement of "legitimate public policy objectives," which, as one of the exceptions, is a reasonable manifestation of the "self" space in data sovereignty; Second, the relevant measures must not constitute "arbitrary or unjustifiable discrimination." Secondly, the measures must not constitute "arbitrary or unjustifiable discrimination"or "disguised restrictions on trade". A "necessity test" has also been included. Restrictive measures imposed by member states must be reasonably related to the policy objective they pursue and must not go beyond what is necessary to achieve that objective,

ISSN: 2710-0170

reflecting the concrete application of the principle of proportionality in the field of data governance and helping to regulate the regulatory behaviour of member states.

However, the limitations of RCEP data flow regulation are also worth exploring. First, despite the existence of a "double standard of review", the lack of focus on "legitimate public policy objectives" makes it difficult for parties to meet the requirements, and the vague formulation of the concept magnifies the possibility that restrictions on the cross-border flow of data may result in arbitrary or unjustified discrimination. At the same time, the application of security exceptions is too biased in favour of parties' regulatory autonomy.

Secondly, there is no unified standard for data classification and grading, so the risk assessment of cross-border data flow lacks an objective basis. Furthermore, the regulation of data localisation measures is relatively insufficient, which may affect the formation of regional data factor markets. Substantively, the RCEP cross-border data flow rules reflect the current state of development of regional digital trade rules. Under the tension between data sovereignty and trade liberalisation, the construction of its norms has taken a prudent and progressive approach, reserving development space for the improvement of the regional data governance system. With the deepening of regional digital economy integration, further refinement and improvement of RCEP cross-border data flow rules will become an inevitable trend.

4.2. Analysis of data flow efficiency from a legal economics perspective

The key to analysing the efficiency of cross-border data flow under the RCEP framework from the perspective of legal economics is to go beyond the limitations of the traditional "Pareto efficiency" and adopt the "Kaldor-Hicks efficiency" standard to construct the institutional framework. "Pareto efficiency" emphasizes the simplicity and feasibility of the law and respects the will of individuals, while "Kaldor-Hicks efficiency" pays more attention to compensation and the overall interests. In this perspective, the efficiency assessment of cross-border data flow regulation needs to consider both short-term and long-term effects. In the short term, the regulatory framework directly affects the cost-benefit structure of data flows: on the one hand, it increases compliance, technology, and operational costs, and on the other hand, it brings direct benefits such as market access and data value release. In the long term, the regulatory framework creates significant institutional benefits, including increased legal certainty, enhanced risk controllability, and increased market trust, and these institutional improvements ultimately drive the overall efficiency of cross-border data flows. This all-encompassing approach to efficiency assessment reveals a seeming paradox: while strict data protection regulation increases compliance costs for businesses in the short term, it actually improves the long-term efficiency of cross-border data flows by creating a predictable legal framework and reducing the risk of data misuse (Figure 1).

However, the fragmentation of data protection laws among RCEP member countries has led to the coexistence of multiple regulatory standards in the region, and the efficiency loss arising from such institutional divergence has exceeded the scope of compensation that can be afforded by individual market players. Promoting the harmonization of regional data protection rules based on the "Kaldor-Hicks" efficiency standard will result in significant efficiency improvements, which will reduce the compliance costs of market players and provide stable expectations for cross-border flow of data elements through institutional innovation and ultimately realise the overall benefits of regional digital economy integration.

ISSN: 2710-0170

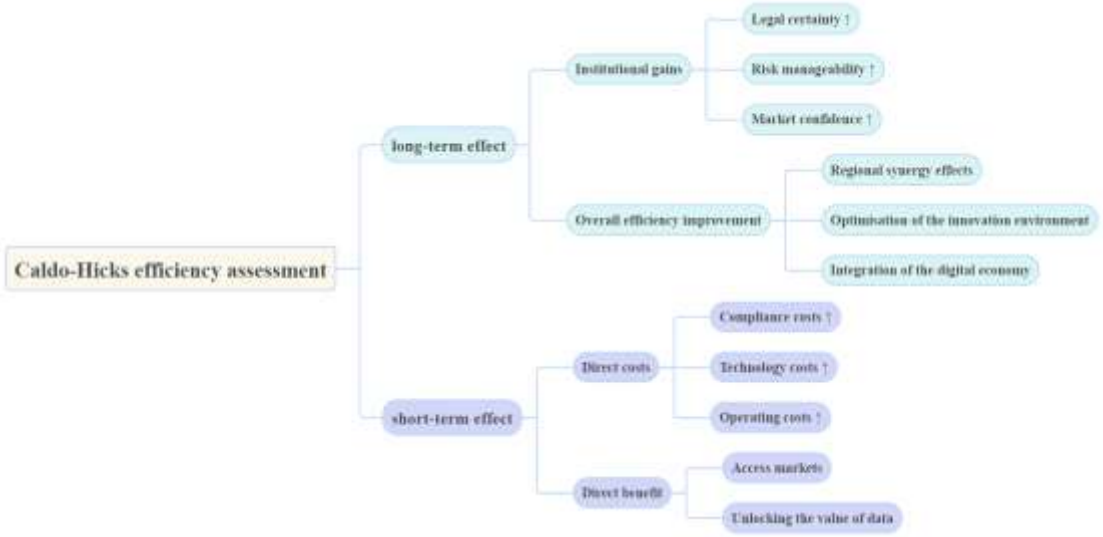

Figure 1 Framework for analysing data flows based on Kaldor-Hicks efficiency

5. Exploration of Practical Paths of Conflict and Harmonisation of Legal Regulation of Cross-Border Data Flows in RCEP

5.1. Multidimensional Analysis of Conflict of Laws on Cross-Border Data Flows in RCEP

Under the RCEP framework, cross-border data flows are faced with multi-dimensional legal conflicts, which reflect the dilemma of applying traditional legal norms in the face of the special attributes of cross-border data element flows. The overlapping jurisdictions, ambiguities in the application of laws, and frictions in the enforcement mechanisms together constitute the key legal challenges constraining the free flow of data elements under the RCEP (Figure 2), which need to be resolved urgently through deep governance changes.

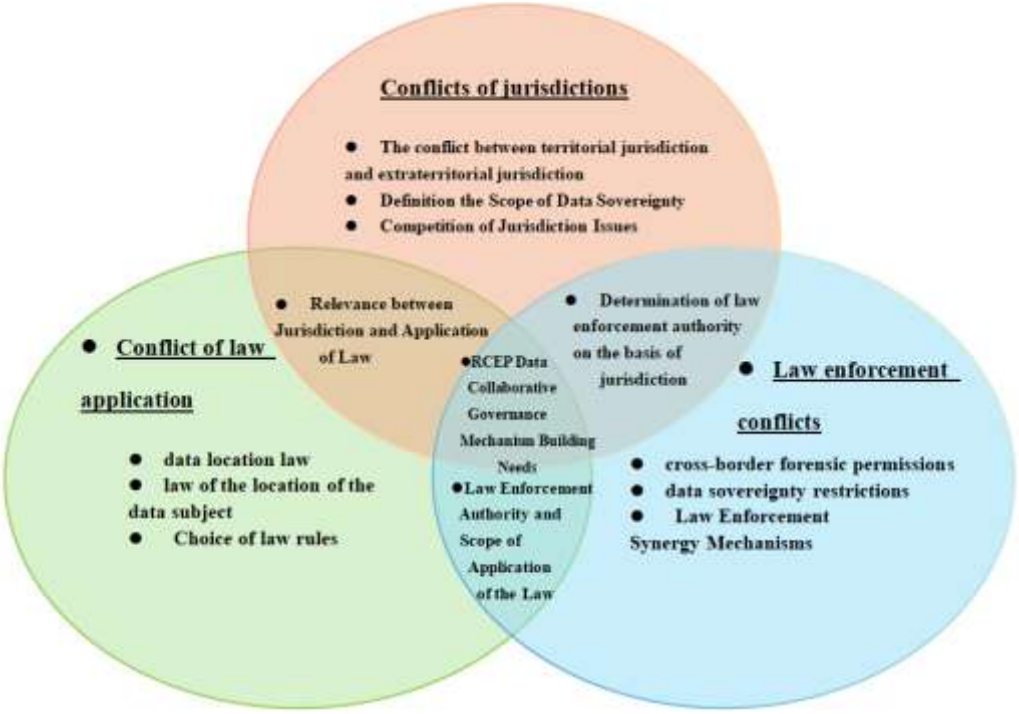

Figure 2 Relationship between jurisdiction, application of law and conflicts of law enforcement

ISSN: 2710-0170

5.1.1. Conflicts of jurisdiction: territoriality versus extraterritoriality

From a procedural law perspective in the area of cross-border data flows, jurisdiction centers on which state has full and effective physical control over the data in flow. The unique ease and arbitrariness of data transmission leads to the fact that in the course of the flow, several countries may have jurisdiction over it based on territorial or extraterritorial jurisdiction. The jurisdiction model of data flow established by each country will inevitably be based on the maintenance of its own interests, and when it comes to cross-border data flow, it is inevitable that countries will have conflicts of interest, which will be manifested as conflicts of jurisdiction. And the special attributes of data and the different considerations of RCEP member states on digital colonialism also lead to the virtualization of the boundaries of data sovereignty, which is further embodied in the heterogeneity of national legislations, and some countries technically through the incorporation of the principle of effect into the provisions of extraterritoriality, as well as the trial court's purposive interpretation of the provisions in dealing with the jurisdictional conflicts involving the extraterritorial protection of data under digital platforms, and other means, indirect extension of jurisdiction, leading to competing jurisdictions.

5.1.2. Conflict of laws: the law of the location of the data versus the law of the location of the data subject

In the field of substantive law, based on the different requirements of data sovereignty and national security of each country, there are differences in the relevant data law regulation, and in the process of cross-border flow of data, once a problem arises and judicial intervention is required, the court will have to face a conflict of law and weigh the law of the location of the data and the law of the location of the data subject. The term “data subject” first appeared in Article 4 of the EU’s General Data Protection Regulation (GDPR), which states that “personal data means information relating to any identified or identifiable natural person (‘data subject’)”. Due to the differences in the relevant rights and obligations stipulated in different jurisdictions, the results of the applicable law will subsequently be very different, and the RCEP does not have a unified provision on this, which involves the rules of law, and the issue of legal application will become more prominent with the continuous development of digital trade and the continuous improvement of the digital regulations of various countries.

5.1.3. Law Enforcement Conflicts: The Tension Between Cross-Border Forensics and Data Sovereignty

The complexity of cross-border forensics, due to the multiple jurisdictions and international cooperation relationships involved, often requires bilateral or multilateral assistance, which leads to questions of competence in cross-border forensics. When compelling service providers to provide data, law enforcement authorities and their geographically limited investigative powers encounter complex and unresolved sovereignty issues, and mutual legal assistance is considered cumbersome and slow. Some foreign scholars define data sovereignty as state law enforcement intervention and judicial sovereignty jurisdiction where data are subject to the laws of the country where they are created and stored. Countries have different degrees of privacy protection based on the importance they attach to sovereignty, and the degree of permissibility of cross-border e-discovery varies greatly, and the process of forensics, if not handled properly, may lead to diplomatic incidents. Objectively speaking, the maintenance of data sovereignty requires the law as a shield, while the current maintenance of data sovereignty hinders the law enforcement process. The solution to this contradiction lies in the construction of a law enforcement synergy mechanism. How to find a balance between cross-border law enforcement and data sovereignty, and how to build a law enforcement coordination mechanism, is also a problem for RCEP.

ISSN: 2710-0170

5.2. RCEP Legal Harmonisation of Cross-Border Data Flows: Exploring Practical Paths for TNCs

In RCEP cross-border data flow legal coordination, multinational corporations, as the main participants in regional data flow and the forerunners of institutional innovation, can most intuitively reflect the implementation effect and optimization direction of the data governance rules under the framework of RCEP in their practical exploration. In particular, the current data regulatory requirements of RCEP member countries are diversified, and the institutional innovations of multinational corporations in this regard provide valuable practical materials for the improvement of regional data governance mechanisms. From the practice of typical multinational companies, Microsoft Azure has set up local data centers specifically for ASEAN, Japan, and South Korea and developed data storage solutions that meet the regulatory requirements of each country, realizing the organic unity of data localization and regional synergy; South Korea's NAVER has created the "Distributed Data Sovereignty Architecture", which has been used in the RCEP and is now used in the RCEP. South Korea's NAVER has created a "Distributed Data Sovereignty Architecture" to achieve dual-track operation of localized processing of sensitive data and regional circulation of non-sensitive data within the RCEP region; Chinese enterprises have also demonstrated excellent compliance and innovation capabilities under the RCEP framework, such as ByteDance, which has built a precise data grading and classification system and ensured regional compliance through a strict risk assessment mechanism, and Ali Cloud and Huawei Cloud, which have actively cooperated with international certification bodies to ensure that they are in compliance with the RCEP region. Aliyun and Huawei Cloud have actively cooperated with international certification organizations to establish a data compliance system that meets the requirements of each member state in the RCEP region. These practical innovations reveal the key path to data compliance under the RCEP framework: building a hierarchical data governance structure through in-depth understanding of the characteristics of regional rules and achieving synergy of the rules with the help of technological means, thus providing a practical paradigm for the improvement of the RCEP data governance mechanism. Practice shows that it is possible for enterprises to achieve a strategic balance between data sovereignty protection and regional circulation through innovative system design and technology application under the existing RCEP rules framework.

6. Optimising the Legal Regulation of Cross-Border Data Flows under RCEP: Towards a Synergistic Governance Mechanism

6.1. Legislative synergies: interaction between framework agreements and domestic law

Legislative synergy, as the primary path for optimizing the legal regulation of cross-border data flows in the RCEP, is the basis for the operation of the synergy system (Figure 3). A new multi-

ISSN: 2710-0170

level regional data governance order should be constructed through the interaction of the framework agreement and domestic laws.

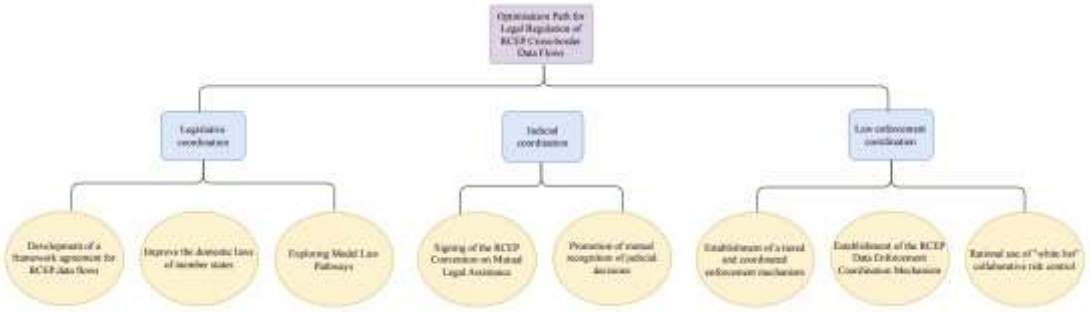

Figure 3 RCEP Cross-border Data Flow Collaboration System Map

First, the RCEP data flow framework agreement should be formulated to clarify the basic principles and rules. The agreement should uphold the core concept of "inclusiveness and openness, innovation and integration, and cooperation and common governance" and create a new paradigm of regional rules and cooperation in the strategic balance between data sovereignty and digital economic development. Specifically, on the one hand, "rule-led, technology-enabled, mechanism-innovation" is the basic path to build both universal and regional characteristics of the normative system; on the other hand, through the "hierarchical classification, risk-orientation, differentiated policy" system design, we can achieve the organic unity of data security and flow facilitation. On the other hand, through the system design of "grading, classification, risk orientation, and differentiated policies", the organic unity of data security and flow facilitation can be achieved; at the same time, through the operation mechanism of "government-led, multi-participation, and collaborative governance", the effective implementation of the framework agreement can be ensured. Secondly, member states should actively improve their domestic legal system, fill legal gaps, and eliminate institutional obstacles. To fill the legal gaps, a complete normative system covering data classification, cross-border flow, security protection, and other core issues should be established; to eliminate institutional barriers, it is necessary to focus on key areas such as data localization requirements, privacy protection standards, security review mechanisms, etc., and to establish a domestic implementation mechanism that is in line with the Framework Agreement. Currently, China's cross-border data legislation includes, but is not limited to, the Network Security Law, the Data Security Law, and the Personal Information Protection Law. Of this legislative "troika", the latter two laws are typical, supplemented by the Regulations on the Security Protection of Critical Information Infrastructure and Measures for the Assessment of the Security of Data Exiting China, constituting the legal framework for the regulation of the cross-border flow of data in China. The latter two laws are typical of the "troika", supplemented by the Regulations on the Security Protection of Critical Information Infrastructure and the Measures for Security Assessment of Data Exit, which constitute the legal framework for the cross-border flow of data in China. Further, in order to promote the soft harmonization of regional data laws, the establishment of an RCEP model law on data governance can be explored, drawing on the UNCITRAL model. The model law should focus on providing legislative models, clarifying normative standards, and setting implementation guidelines, so as to provide a reference for member states to improve their domestic laws and provide benchmarks for the harmonization of regional rules. Through the multi-level legislative synergy mechanism of "Framework Agreement -Domestic Law - Model Law", it can further ensure that the data sovereignty of each country is fully respected, promote the efficient flow of regional data elements, and thus contribute constructive "Asia-Pacific Wisdom" in the process of

ISSN: 2710-0170

reconstructing international rules. This will contribute constructive "Asia-Pacific wisdom" in the process of reconstructing international rules. This institutional structure is in line with the development needs of regional economic integration in the digital era while at the same time highlighting the value of creating new international economic and trade rules and providing inspirational regional practice for the improvement of the global digital trade governance system.

6.2. Judicial synergy: deepening cooperation and building mutual trust

Judicial synergy is a strong guarantee to promote the effective implementation of RCEP, and should promote the deepening of cooperation and mutual trust to build a more efficient and integrated regional judicial system.

Firstly, sign a convention on mutual legal assistance to regulate cross-border evidence collection procedures. The key to clarifying the scope of assistance and procedures of the MLA Convention is to regulate the procedure of cross-border data e-discovery to ensure fairness and authority. Firstly, to ensure that forensics are executed under the framework of mutual legal assistance. Secondly, uniformly construct efficient and convenient forensic procedures. On the one hand, simplify the evidence collection process, provide for direct cooperation between the law enforcement agencies of the requesting and requested countries in the "one-word" evidence collection process, and at the same time reduce the review process of the interested countries to ensure that the evidence is real and effective. On the other hand, explore the establishment of electronic mutual legal assistance procedures to improve the efficiency of evidence collection. In addition, the path of "public-private cooperation" in evidence collection should be clarified, and network service providers should be actively mobilized to provide more comprehensive data, respecting the status of private subjects and supporting relief systems.

Secondly, promote mutual recognition of judicial judgments to improve judicial credibility. On the one hand, through the issuance of the RCEP Joint Interpretative Procedural Rules, the judicial interpretation regulations can be realized to formulate uniform mutual recognition and enforcement standards, standardize the review procedures and conditions, and reduce conflicts in the enforcement of judgments due to the inconsistency of the standards. On the other hand, regional judicial exchanges and mutual visits should be strengthened on a regular basis to promote the broad participation of member states in judicial governance and enhance the quality and efficiency of international commercial trials. At the same time, it has built a monitoring mechanism for judicial assistance, standardized the jurisdiction system of commercial courts, established a review body, and regularly assessed the effectiveness of the implementation of judicial cooperation strategies.

6.3. Law enforcement synergy: institutional innovation and capacity-building

Law enforcement synergy is a key step in ensuring the effective operation of synergistic mechanisms, and institutional innovation and capacity-building should be strengthened to ensure the smooth operation of the rule of law track of regional data.

Firstly, a layered and coordinated enforcement mechanism should be established. Taking the RCEP e-commerce norms as the overarching principle, a special data flow management committee should be set up at the regional level, responsible for formulating unified law enforcement standards and coordinated rules; at the bilateral level, direct law enforcement collaboration agreements should be established among member countries to clarify specific issues such as jurisdiction division, evidence admissibility, and penalty convergence; at the domestic level, each member country should improve its own data governance regulations to eliminate conflicts with regional rules. Secondly, in terms of organizational structure, a "matrix" synergy network should be established to create a "specialized and regionalized" law enforcement coordination mechanism. A permanent regional joint enforcement office should

ISSN: 2710-0170

be set up to coordinate cross-border enforcement actions; an expert advisory committee should be established to provide professional support for complex cases; a joint investigation team should be formed to deal with major cross-border data violation cases; and the RCEP secretariat should be set up and operated as soon as possible. To promote the dissemination of information and to provide dispute resolution support. At the same time, we should strengthen the construction of expert committees and joint investigation groups and carry out joint enforcement activities to deal with major cases. Finally, the "whitelist system" should be used reasonably to carry out coordinated risk control. Member States should rationally allocate enforcement resources in accordance with the whitelist to improve enforcement efficiency. They should also unify the whitelist entry criteria and review and update mechanism and adopt limited "data controller criteria" to access cross-border data for classification and review, so as to avoid unfair and insufficient law enforcement.

7. China's Policy Innovations in the Legal Regulation of RCEP Cross-Border Data Flows Paths and Options

As an important member of RCEP and a world trade power, China has the dual role of market supplier and final demander in RCEP. Currently, China's cross-border data flow regulation is a data territorial regulation model that gives priority to national security, and it should, on the basis of its existing experience, further converge with the RCEP agreement and become a rule maker, a balancer of interests, a leader in innovation, and a bridge to promote win-win cooperation.

7.1. Institutional innovation: Towards a new paradigm of differentiated regulation

Institutional innovation in China's RCEP Cross-border data flows should be based on the value of data, and a risk-oriented classification and grading regulatory system should be constructed to form a new paradigm of differentiated regulation. This regulatory paradigm breaks through the traditional "one-size-fits-all" regulatory thinking and aims to build a dynamic regulatory mechanism in line with the digital era.

Firstly, in the dimension of risk control, a sandbox regulatory mechanism has been innovatively introduced, and a risk warning and exit mechanism has been formed using the sandbox pilot mode. Second, in the dimension of data classification, according to the special characteristics of cross-border data flow, it is divided into three types of scenarios, namely, "basic flow", "high-frequency flow" and "complex flow". Basic flow is mainly related to regular trade data, adopting the "negative list + ex post facto supervision" mode; high-frequency flow is aimed at transaction data and user data in digital trade, implementing the "hierarchical filing and real-time monitoring" mechanism; complex flow covers emerging technologies, Complex flows cover emerging technologies, industrial chains, and other strategic data, and implement the strategy of "full review-continuous assessment". Thirdly, in the dimension of data grading, a three-dimensional assessment system of "sensitivity-frequency of flow-security risk" has been established, and differentiated supervisory measures have been adopted for data flows of different risk levels.

7.2. Mechanism innovation: building a multi-level synergistic governance framework

The key to innovative collaborative governance mechanisms lies in the construction of a multilevel collaborative governance framework with vertical and horizontal synergies and internal and external linkages.

In the construction of the vertical and horizontal synergistic governance framework, in the vertical dimension, it is necessary to form a three-tier linkage mechanism: the central level

ISSN: 2710-0170

establishes a cross-border data governance committee to coordinate the formulation of policies and strategic coordination; the departmental level establishes a joint conference system for data regulation, integrating the functions of departments such as Netcom, industry information, commerce and customs, so as to achieve the organic unity of data security, trade facilitation and industrial development; the local level establishes a cross-border data authority to carry out localised regulatory innovations. organic unity of data security, trade facilitation, and industrial development; and the establishment of cross-border data management bureaus at the local level to carry out localized regulatory innovation. In the horizontal dimension, it is necessary to establish a four-party synergy system of "government-enterprise-agency-platform": the government is responsible for top-level design and regulatory control, enterprises are involved in standard-setting and practice innovation, professional organizations provide technical support and risk assessment, and digital platforms are responsible for data governance and flow control.

Internal and external linkages should be promoted to build a regional integration framework. On the one hand, it is necessary to build a compatible regulatory framework and advocate the establishment of an RCEP data flow dispute resolution centre. Regarding the choice of model for the RCEP dispute settlement mechanism, China should insist on adopting a pluralistic settlement model. At the same time, special arrangements should be made for different advantageous areas by designing the areas covered by the dispute settlement mechanism. On the other hand, China should form bilateral and multilateral cooperation modes and build a regular communication mechanism among RCEP member countries. The key to bilateral and multilateral cooperation is to promote the docking and mutual recognition of internal and external regulatory standards. China should standardize and publicize the classification standards for important data, and at the same time, establish a multi-level dialogue mechanism to promote the sharing of information, such as encouraging China's FTZ pilots to carry out exchanges with member countries to form a regular communication channel. This governance framework breaks through the traditional one-way control model, promotes the overall enhancement of regulatory effectiveness, and provides a Chinese program for the innovation of regional digital governance mechanisms.

7.3. Technological innovation: creating a new model for secure data flows

Technological innovation is an important driver for the effective implementation of RCEP-related agreements and laws, and technological innovation should focus on constructing a new governance model of "secure and controllable, credible authentication, and dynamic protection", and the core innovation path is to build a technological system of protection and synergy. At the protection level, firstly, the implementation of basic-level technical protection, using data encryption, data desensitization, authority control, deployment of firewalls and other means to enhance the degree of protection of private data. Second, using decentralization and data sharing to form a digital identity mutual recognition credit mechanism, encrypting, tracking and verifying data flowing across borders to ensure its security and transparency, and enhancing the degree of trust in cross-border trade. Third, relying on federated learning, under the premise that the data itself does not move, multi-party joint data to establish a virtual common model, optimize privacy algorithms, avoid unauthorized data proliferation, share cross-border data value, and realize the data" "available but not visible", to improve data security. At the collaborative level, it is necessary to build standardized data interfaces and transmission protocols to realize the interconnection and interoperability of data flows among RCEP member countries; build digital risk situational awareness systems to realize real-time monitoring and early warning of cross-border data security; and deploy networked emergency response and collaboration platforms to support the rapid response and joint handling of cross-border data security incidents. The breakthrough of the technological innovation system is to

ISSN: 2710-0170

promote the transformation from passive defense to active protection, build a new mode of data flow with both security and efficiency, and provide solid technical support for the development of RCEP digital trade.

Acknowledgements

This study is a result of the Beijing Union University Qimingxing Project “Investigation and Research on Personal Financial Data Security Risks and Legal Policies Driven by Technological Innovation”(Project Number: 20051043).

References

[1] Congjing Ran and Yan Liu: A theoretical genealogy of data sovereignty, Journal of Wuhan University (Philosophy and Social Science Edition),75(2022)No.6,p.24.

[2] Xiang Sheng, Lin Yu and Haiying Huang: Cross-border data localization: sovereignty considerations, security bottom line and strategic positioning, Library Forum,43(2023)No.9,p.22.

[3] Martina Francesca Ferracane: Data flows and national security: a conceptual framework to assess restrictions on data flows under GATS security exception, Digital Policy Regulation and Governance,21(2019)No.1,p.47.

[4] Zhipeng He and Tianjiao Shen: Exploring the effectiveness of international soft law in global governance, Academic Monthly,(2021)No.1,p.111.

[5] Chengyu Zhang: RCEP Basic Security Exceptions for Cross-Border Data Flows and China's Response, Journal of Education, Humanities and Social Sciences,14(2024),p.39.

[6] Gui Huang and Yin Lei: The Norms on Cross-Border Data Flows in the RCEP, Asian Journal Of Law And Economics,(2022)No.3,p.384.

[7] Yuqiong Du and Xinyu Luo: The Application of the Exception Clause of the RCEP Data Cross-border Flow Rules and China's Response, Journal of Sichuan Normal University (Social Science Edition),(2023)No.5,p.77-78.

[8] Bo Feng, Yang Tong: The Origin and Difficulties of Legal Economics, Journal of Zhejiang University (Humanities and Social Sciences Edition),47(2017)No.4,p.230.

[9] Kang Yuan and Wanru Zhao: Jurisdictional conflicts and their coordination in cross-border data flow, Journal of Chongqing University of Posts and Telecommunications (Social Science Edition), (2024)No.2,p.67-68.

[10] Congjing Ran, Guirong Chen and Huan Wang: Study on the Manifestation of Jurisdictional Conflicts of Cross-border Data Flows in Europe and the United States and the Main Solution Paths, Library and Intelligence, (2020)No.3,p.78.

[11] Zhiqi Zhou: A case study of extraterritorial jurisdictional boundaries of data under global legal practice: balancing interests in expansion and contraction[J]. Journal of International Economic Law, (2023)No.4,p.46.

[12] Paul de Hert,Cihan Parla and Juraj Sajfert: The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders. Unilateralist transborder access to electronic evidence promoted via soft law, Computer Law & Security Review, (2018)No.2,p.328.

[13] Bin Liao and Minxian Liu: Research on cross-border electronic data forensics under data sovereignty conflict, Journal of Law, (2021)No.8,p.149.

[14] Xuebo Zhang and Zhitao Wang: RCEP data cross-border flow rules and China's data cross-border flow legislation, SAR Practice and Theory, (2024)No.1,p.100.

[15] Junwei Feng: Development and reflection of cross-border e-discovery system, Journal of Law, (2019)No.6,p.34.

[16] Guangxi Wei and Xiangshu Liu: Specific path of public-private cooperation in cross-border data forensics, Journal of the People's Public Security University of China (Social Science Journal), (2024)No.1,p.70.

ISSN: 2710-0170

[17] Fulin Chi: Comprehensive and high-quality implementation of RCEP requires joint efforts of all parties (Observatory), People's Daily (Overseas Edition), 2024-9-7.

[18] Chen,Meng. Developing China's Approaches to Regulate Cross-border Data Transfer: Relaxation and Integration, Computer Law & Security Computer Law & Security Review, (2024)No.54,p.10.

[19] Mingyue Liao, Jiayi Wang and Yingxue Yang: Security risks in cross-border enforcement of US CLOUD Act data and China's response, Library Forum, (2024),p.8.

[20] Jun Sun: China's Role and New Development Pattern in RCEP, Academic Forum, 46(2023)No.2,p.61.

[21] Xi Wang and Jinhan Gao: Research on the Construction of RCEP Dispute Settlement Mechanism, International Outlook,10(2018)No.2,p.150.

[22] Qiang Yang: AI and data privacy protection: A crack at federated learning, Information Security Research,5(2019)No.11,p.963.

[23] Pengfei Wang, Zongzheng Wei and Dongsheng Zhou et al: A review of federated forgetting learning research, Journal of Computer Science,47(2024)No.2,p.398.