

RESEARCH ARTICLE

The Dilemma of Cross-Border Data Flow and the Construction of Mutual Trust Platform in Asia

Zerui Zhao 

China Institute for Socio-Legal Studies, Koguan School of Law, Shanghai Jiao Tong University, Shanghai, China

Email: ruczr@sjtu.edu.cn

Abstract

The current unilateral and bilateral governance agreement cannot solve problems such as the large strength gap, loose organisation, and cultural diversity in cross-border data flow in Asia. Therefore, we are in urgent need of structuring a multilateral governance mechanism, that is, to build a mutual trust platform for cross-border data flow in Asia. From a digital technology perspective, the Asian Cross-Border Data Flow Trust Platform is a blockchain-based digital technology architecture. From the perspective of the organisational model, the Asian cross-border data flow governance based on the mutual trust platform can be understood as a cooperative network in which multiple Asian countries cooperate to make cross-border data decisions. As a necessary medium to eliminate the complexity of the cooperation network, legal procedures will transform the chaos on the Asian Cross-Border Data Flow Mutual Trust Platform into order by simplifying the communication between multiple agents.

Keywords: data cross-border; mutual trust; platform; Asian regional integration

1. Introduction

The continuous trade conflict between China and the United States, along with the global epidemic of the novel coronavirus, not only seriously damaged the economic development of various countries, but also continuously harmed the trade relations among them. In order to achieve rapid economic recovery, the world has begun to promote the digital transformation of society. The digital economy, fuelled by data and algorithms, is becoming the focus of global attention. However, the emergence of new risks, such as cyber security and the digital divide, makes it difficult for digital technologies that could strengthen global trade relations to play a structural role in cross-border trade. How can we promote the cross-border flow of data while ensuring the security of national networks and data, so as to integrate into regional and world economic development and achieve the mutual benefit and win-win results of the digital economy? This has become a common problem for national governments and regional economic organisations (Cate, 1999, pp. 173–176). However, due to differing governance concepts and needs, countries around the world have formed vastly different data governance policies. The negotiation and formulation of digital trade rules under the framework of the World Trade Organization is slow and difficult to operate within a short period (Gao, 2018, pp. 297–321).

In this context, most scholars concerned with cross-border data flow focus on the policies of the EU and the US, as well as related regional digital trade agreements, trying to

find a suitable path for cross-border data governance. However, because the current situation of the digital economy, the foundation of social trust, and the data governance concepts of Asian countries differ from those of the EU and the US, it is difficult to replicate the data governance policies and regional data trade agreements to build effective cross-border data governance mechanisms that meet the actual needs of Asia. Compared with the cross-border data governance research in the EU and the US, the research in Asia is obviously insufficient. This makes it difficult for Asian countries to achieve the regional integrated development of the digital economy, and thus increases the likelihood of missing the opportunity to use digital technology to help the Asian economy achieve inclusive and sustainable development.

After the background introduction in the first section, this paper will describe the development status and potential of the Asian digital economy in Section 2, and reveal the institutional barriers to the cross-border data flow in Asia by combing the current cross-border data governance policies of Asian countries. On this basis, Section 3 will combine the status quo of cross-border data flow in Asia, guided by the EU and the US, to point out the uniqueness of cross-border data flow in Asia, and demonstrate the necessity of building a mutual trust platform for cross-border data flow in Asia. Section 4 will further point out the technical basis, conceptual support, and legal guarantee for building a mutual trust platform for cross-border data flow in Asia, trying to combine digital technology, platform governance, and legal procedures to solve the problem of cross-border data flow in Asia.

2. The development status and institutional obstacles of the Asian digital economy

2.1 The development status and potential of Asia's digital economy

The novel coronavirus outbreak in 2019 is driving the digital transformation of companies around the world. The digital economy, led by digital platform companies such as digital media, e-commerce, e-services, online travel, advertising technology, and digital transportation, is constantly promoting output, trade, and employment growth in countries around the world. For Asian countries in particular, digital transformation will help them overcome challenging geographical environments, provide opportunities for them to participate in international trade and move up the value chain, strengthen transnational trade in Asia, and help to achieve cross-regional and inclusive development of the Asian regional economy. According to data released by the Asian Development Bank in 2021 (see Table 1), global digital economy revenue reached \$3.8 trillion in 2019, equivalent to 4.4% of global GDP. E-commerce accounts for more than half of that revenue (about \$1.9 trillion), of which about \$1.1 trillion comes from Asia. In 2019, Asia's digital economy grew faster than other economies, including the US and Europe, at 16.1%, while global growth was just 12.7%. Asia is leading the digital economy in all areas except for advertising technology (such as Google and Facebook). In the e-commerce sector, Asia accounts for more than 58% of total sales revenue.

However, as the Asian countries in the digital transformation of social security concerns increasingly intensified, countries have issued laws and regulations for the problem of cross-border data flow but lack communication and coordination channels, leading to distrust in cross-border data flow between governments in Asia, and the cross-border trade costs for Asian companies increased significantly. Such differences and uncertainties in the laws and regulations of cross-border data flow in Asia will become the main factors hindering the regional integration and development of the digital economy in Asia.

Table 1. Digital economy revenues and growth—world and Asia, 2019 (\$ million)

Type of digital economy	Asia Revenue – Growth rate	World Revenue – Growth rate
Digital media	\$67.6 million	\$177.5 million
e.g., iQiyi, Sea, Bilibili	– 7.1%	– 6.3%
e-Commerce	\$1,119.2 million	\$1,924.9 million
e.g., Alibaba, Flipkart	– 19.6%	– 16.4%
e-Services	\$71.7 million	\$161.8 million
e.g., Ele.me, Ziroom, Swiggy	– 18.8%	– 16.0%
Online travel	\$379.5 million	\$1003.8 million
e.g., OYO, Ly.com, Traveloka	– 9.1%	– 7.2%
AdTech	\$110.4 million	\$331.7 million
e.g., Bytedance, Tencent	– 14.3%	– 14.4%
Transportation	\$75.4 million	\$190.3 million
e.g., Didi Chuxing, Grab	– 12.4%	– 8.0%
Total	\$1,823.7 million	\$3790.0 million
	– 16.1%	– 12.7%

Sources: Asian Development Bank calculations using data from World Bank. World Development Indicators. Available at: <https://data.banl.worldbank.org/source/worlddevelopment-indicators> (Accessed: July 2020).

2.2 Classification of national laws and regulations on cross-border data flow in Asia and their obstacles to regional development

For the problem of cross-border data flow, national laws and regulations mainly have two aspects: one is which data needs to be strictly restricted on cross-border flow, that is, the rules of data localisation; the other aspect is other legal conditions for cross-border data flow, that is, the rules of cross-border flow of data. Cross-border flow rules of data focus on imposing obligations and responsibilities on third parties of data transmission to ensure the security of cross-border data flow. The localisation rules of data focus more on setting the ban on the flow of specific data abroad and the obligation to store specific data within the borders. (Anupam and Le, 2015, pp. 679–704) From the perspective of cross-border data flow rules and data localisation rules, there are great differences and uncertainties in Asian national laws and regulations on cross-border data flow issues.

There are disagreements on laws and regulations regarding cross-border data flows in Asia. China is governed by an “overall national security concept,” which forms the core of its governance framework. This includes the establishment of the “equal security” governance principle, alongside data exit security assessment procedures and localisation of critical information infrastructure. These elements serve as mechanisms of governance aimed at constructing a joint, sharing, win-win security pathway in Asia, encompassing cooperation security, common security, comprehensive security, and sustainable security initiatives (Xu, 2021, pp. 22–37) (see Table 2).

Japan and Singapore, both applying their core governance concepts of “equal protection,” have created independent regulators and granted them the power to identify countries or regions exempt from compliance. At the same time, Japan and Singapore are also trying to build their own countries into data centres in the Asia-Pacific region by

Table 2. Combing the laws and regulations on cross-border data flow in China

Nation	Rules for the flow of data across borders	Data localisation rules
China	<p>1. Article 38 and 39 of the Personal Information Protection Law: If personal information processors really need to provide personal information outside the People's Republic of China due to business needs, it shall meet one of the following conditions: ① passes the security assessment organised by Article 40; ② passes the national authority; ③ contracts with the overseas receiver for the rights and obligations of both parties; ④ other conditions stipulated by laws, administrative regulations, or national cyberspace authority.</p> <p>Personal information processors shall take necessary measures to ensure that the activities of overseas recipients in processing personal information meet the personal information protection standards stipulated in this Law.</p> <p>Where a processor of personal information provides personal information outside the territory of the People's Republic of China, it shall inform the individual of such matters as the name or names of the recipients outside the territory, their contact details, the purpose of the processing, the manner of processing, the types of personal information, and the manner and procedures by which the individual may exercise the rights provided for in the Law to the recipients outside the territory, and shall obtain the individual's individual consent to do so.</p> <p>2. Measures for Security Assessment of Data Exit: The Measures stipulate the assessment principles of 'risk prevention', 'orderly and free flow in accordance with the law' and 'equal security', and set up two modes of assessment, namely, pre-assessment and continuous supervision. The assessment includes self-assessment (comprehensive assessment) and security assessment. Self-assessment (comprehensive assessment) targets the scale, scope, type and sensitivity of all data, with the objective of ensuring the recipient's safety and security capabilities (management and technical measures, etc.) (certification, etc.). Security assessment, on the other hand, targets the scale, scope, type and sensitivity of the outbound data, with the goal of ensuring that the recipient has sound policies and regulations, a cybersecurity environment and a level of data protection.</p>	<p>1. Article 40 of the Personal Information Protection Law: The operators of critical information infrastructure and the personal information processors reaching the amount stipulated by the cyberspace department of the State shall store the personal information collected and generated within the territory of the People's Republic of China. If it is really necessary to provide it overseas, it shall pass the security assessment organised by the cyberspace department of the State.</p> <p>2. Article 37 of the Cyber Security Law: Personal information and important data collected and generated by the operators of the key information infrastructure in the operation of the People's Republic of China shall be stored in the territory. If it is really necessary to provide it overseas due to business needs, the safety assessment shall be conducted in accordance with the measures formulated by the Cyberspace Administration of the State together with the relevant departments under the State Council.</p> <p>3. Article 31 of the Data Security Law: the exit security management of important data collected and generated by the operators of the People's Republic of China shall apply to the provisions of the People's Republic of China; the exit security management measures of other important data collected and generated in the operation of the People's Republic of China shall be formulated by the State Cyberspace Department together with the relevant departments of the State Council.</p> <p>4. The interim measures for the network taxi booking service management Article 27: network taxi platform company shall abide by the relevant regulations of the national network and information security, the personal information collected and generated business data, shall be stored and used in mainland China, storage period less than 2 years, except as otherwise stipulated by laws and regulations, the information and data shall not be outflow.</p> <p>5. Article 10 of the Measures for the Administration of Population Health Information (Trial): Population health information shall not be stored in servers abroad, and servers shall not be hosted or leased abroad.</p> <p>6. Article 24 of the Regulations on the Administration of the Credit Investigation Industry: The collation, preservation and processing of the information collected by the credit investigation agencies in China shall be carried out in China.</p> <p>7. Article 6 of the Notice of the People's Bank of China on Banking Financial Institutions to Protect Personal Financial Information: The storage, process and analysis of personal financial information collected in China shall be carried out in China. Unless provided for by laws and regulations and the People's Bank of China, banking financial institutions shall not provide domestic personal financial information abroad.</p>

actively establishing bilateral or multilateral agreements for cross-border data flows (Xu, 2020, pp. 185–197) (see Table 3).

India highlights the governance concept of “data localisation,” which requires both personal data and non-personal data to be stored within its borders; adopts hierarchical control for different types of data; and sets stricter localisation requirements for key personal data and sensitive personal data. In addition to meeting national needs and strict localisation requirements, India has set up diversified regulatory mechanisms and exemption rules to create space for cross-border data flow. Enterprises can choose cross-border data flow regulatory mechanisms suitable for their businesses, and the central government has the right to exempt part of the data localisation requirements (Hu and Kong, 2019, pp. 306–310) (see Table 4).

Vietnam and Indonesia have not yet developed a unified governance system, with rules for cross-border data flow for personal data and data localisation rules on specific categories of data. South Korea is more conservative, allowing only personal data to flow overseas under temporary circumstances, and with the consent of the data subject. However, South Korea also lacks review of the protection measures and protection of mobile destinations (see Table 5).

At the Asian Business Conference, national business representatives argued that the diversity of laws and regulations on cross-border data flow is the biggest challenge for Asian multinational companies in the compliance process (Dai, 2021, pp. 119–138). Because the cross-border data flow compliance process of Asian multinational companies will inevitably involve multiple jurisdictions, this will lead to high costs associated with their applicable regulations, risk assessment, and regional operations. In the current divergence of laws and regulations among Asian countries, multinational companies need to ensure that their consent mechanisms can be recognised and effectively implemented in all jurisdictions involved. This disguised requirement necessitates that enterprises establish complex selection steps in the consent mechanism for data flow, which will severely affect user experience and limit transactions. Such differences would also compel multinational companies to produce a comprehensive, lengthy package of consent forms full of legal terms. According to research, a user who legally reads data use and privacy policies would incur productivity losses of \$781 billion if they read all the sites they visit within a year (McDonald and Cranor, 2008, pp. 543–568). At the same time, the incompatibility of laws and regulations on cross-border data flows among Asian countries will also stifle corporate innovation, limit investment in digital technology, and reduce potential social benefits.

In terms of the uncertainty of laws and regulations on cross-border data flow in Asia, the current legislation in Asian countries does not stabilise expectations regarding compliance requirements for cross-border data flow. First of all, the compliance requirements lack transparency and predictability in the laws of different countries, and it is difficult for these countries to reach a consensus understanding of the compliance requirements in the laws of others, which makes enterprises face great uncertainty when applying the laws and regulations in many jurisdictions. Second, Asian countries continue to introduce new laws and regulations on cross-border data flow, and constantly sign bilateral or multilateral agreements with other countries, which makes enterprises face huge mechanism adjustment costs. In many countries involved with multinational enterprises, whenever a country has sent a change in its cross-border data flow rules, it must readjust its data protection mechanisms and obtain user consent. Moreover, the uneven judicial efficiency among Asian countries makes it difficult for enterprises to maintain stable expectations for the application of these laws and regulations, and the lack of communication and coordination among countries even leads to the problem of multiple penalties and repeated accountability.

Therefore, in order to promote cross-border data flow in the Asia region and realise the regional integrated development of the Asian digital economy, Asian countries must

Table 3. Combing through the laws and regulations on cross-border data flows in Japan and Singapore

Nation	Rules for the flow of data across borders	Data localisation rules
Japan	<p>1. The Personal Information Protection Law: After the revision in 2016, the law requires cross-border data flows to obtain the prior consent of data subjects before providing personal data to overseas third parties. Of course, the law also provides two exceptions without user consent: ① provides user personal information to a third party identified by the Japanese Personal Information Protection Commission (“PPC”) as having the same level of personal information protection as Japan (the “whitelist country”); ② meets the following criteria in the rules set by the PPC: a. Institutional design based on the contract between the information provider and the receiver (similar to the Standard Contract Clause in the EU Data Regulation (GDPR)) or the same group as the receiver and established internal rules and privacy policies applicable to both parties (institutional design similar to the Binding Company Guidelines in GDPR); b. The information recipient has been certified by the international system of personal information processing, such as the APEC Cross-border Privacy Rule System.</p> <p>2. After the Japanese Personal Information Protection Act (revised 2020) took effect on 1 April 2022, the latest version adds two new requirements for cross-border data circulation: ① shall disclose the personal information protection system in the country of the information recipient; ② takes necessary measures to ensure that the overseas third party continuously implements protection measures comparable to the Act on the Protection of Personal Information protection requirements for personal information, and can provide information on the necessary measures taken by the enterprise under the data subject requirements.</p>	<p>1. Japan's Anti-Unfair Competition Law, Pointers on Limited Data Supply, Contract Guide for Artificial Intelligence and Data Utilization, Introduction to Data Utilization, Data Utilization Opinions Set and Data Utilization Cases Set try to build a systematic “limited data supply” protection system. Limited data provided refers to the technical information or business information provided to specific people for the purpose of business, accumulated a considerable amount by electromagnetic-methods, conducted electromagnetic management (except as secret management). The relevant system of “trade secrets” aims to protect the information managed by operators from improper use; and the relevant system of “limited data provision” aims to protect the information provided to certain persons from improper use under certain conditions.</p>

(Continued)

Table 3. (Continued)

Nation	Rules for the flow of data across borders	Data localisation rules
Singapore	<p>1. Article 26 of the Personal Information Protection Act: “personal information flow across Singapore” provisions: ① for cross-border flow of data, institutions shall establish in accordance with the law, to ensure that the flow of data is equal to the Singapore law of protection, otherwise the cross-border flow shall not be conducted in Singapore. ② the Singapore Personal Information Protection Commission may, upon application by the agency, notify the waiver of the aforementioned cross-border compliance obligations in writing. ③ the available circumstances of exemption may be stated in writing by the Personal Information Protection Committee; the exemption does not need to be published in the Government Gazette and the Commission may revoke it at any time. ④ the Personal Information Protection Commission of Singapore may increase, change or revoke the specific application of the exemptions at any time.</p> <p>2. The Key Concepts Advisory Guide 19.5 stipulates the “Cross-border data flow contract terms”: the proposed contract shall require the data recipient to meet no less than the level of data protection stipulated in the Personal Data Protection Act. The contract must cover the following terms: for the data intermediary, there must be protective measures and retention period; for organisations except the data intermediary, there must be provisions on regulating the collection purpose, utilisation and disclosure; ensure the accuracy, protective measures, retention period, data protection policies, data acquisition, correction, etc.</p>	<p>There is no legal requirement for data storage in Singapore. That is why the establishment of one or several cross-border data centres for data storage, processing, trading, and mobility activities is acceptable, as long as institutions comply with the currently applicable laws or regulations on data disclosure and cross-border flows in Singapore. But its Banking Act (Chapter 19) restricts banks’ flow or disclosure of customer information and data to third parties (such as cloud service providers).</p>

Table 4. Review of laws and regulations on cross-border data flows in India

Nation	Rules for the flow of data across borders	Data localisation rules
India	<div><div>1. Information Technology Law: necessary or data subject consent is the premise for the transmission of sensitive personal data or information abroad.</div><div>2. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data and Information) Rules: When transmitting sensitive personal data or information, we must ensure that these legal entities or natural persons can provide the same level of protection of data. Such transmission can only be allowed if it is intended to perform a legal contract between the legal entity or the natural person and the data provider, or if the data provider agrees to conduct the transmission.</div></div>	<div><div>1. Article 4 of the Public Records Act: “No person shall bring any public records out of India without the prior approval of the central government; but obtained or sent for any official purpose.”</div><div>2. Personal Data Protection Act 2018 (Draft): The Data Trustee “shall ensure that at least one copy of the applicable personal data service is stored on servers or data centres in India”, unless the government exercises its authority to designate “certain categories of personal data” as exempt from local storage requirements. In addition, personal data can only flow outside India as required under the Act.</div><div>3. The Personal Data Protection Act 2019 requires companies to store key personal data collected in India before transferring abroad for desensitisation and only for purposes permitted by law.</div><div>4. Draft Rules of Electronic Pharmacy: The data generated through the electronic pharmacy portal shall be maintained locally in India, and shall not be transmitted to or stored outside of India in any way.</div><div>5. India Draft National Policy Framework for e-commerce: There are broad data localisation requirements for personal data and other data, and the “key personal data” identified by the Indian government and the data generated by e-commerce platforms, social media, search engines, and so on can only be stored in India.</div><div>6. The Decree on the Storage of Information on Payment Systems: Providers of payment systems (including intermediaries, payment gateway providers, third-party suppliers, etc.) as recognised by the Central Bank of India are obliged to keep only all information related to the payment system in India.</div><div>7. The Uniform License Act in the Field of Electrical Communications: Electrical communication service operators licensed from the Ministry of Electrical Communications (Department of Telecommunications) shall comply with their domestic data preservation and storage obligations. No flow of financial information (except international roaming and fee information) and user information (except those outside of India who use the Indian operator network in roaming) to the outside of India.</div></div>

Table 5. Review of laws and regulations on cross-border data flows in Vietnam, Indonesia, and South Korea

Nation	Rules for the flow of data across borders	Data localisation rules
Vietnam	<p>I. The Decree for the Protection of Personal Information: The personal information of Vietnamese citizens can flow to the borders and territory of Vietnam when the following conditions of ① to ④ are met (Article 21, (1)). ① data entity agrees to flow; ② original information is kept in Vietnam; ③ gives documents that the country, territory or specific territory has restrictions related to personal information protection equal or higher as specified in this order. In addition to the written approval of the Personal Information Protection Committee, the decree also stipulates that the personal information can be transferred to foreign countries, even if the above ① to ④ conditions are not met (the same as Article 3). data subject agrees to flow; obtains written approval from the Personal Information Protection Committee; exists an information processors to protect personal information; exists a personal information processors commitment to implement means of personal information protection.</p>	<p>I. The network security law of Article 26 item 3: the service provider in the personal information of Vietnam-related data, service user-related data or service user data of the collection, utilisation, analysis or calculation, in the government of Vietnam within a regular period of obligation to keep the data in Vietnam.</p> <p>2. The management, provision, and utilisation of network services and online information order 72 of Article 24 (2), Article 25 (8), Article 28 (2) and Article 34 (2): online service operators in the province of information, for customer complaints related to the provision of the information by the jurisdiction administrative authority to confirm the obligation to set up at least one local server system to deal with the data storage and provision requirements.</p>
Indonesia	<p>I. Provincial Rules of Communication Information 2016 on Personal Information in Electronic Systems No.20 (Minister of Communications and Informatics Regulation No.20 of 2016 on the Protection of Personal Data in an Electronic System) Article 49: Cross-border flow of ① data shall submit a minimum report of the flow destination country, flow other party, flow day, flow reason, ② requests support as needed, and the implementation of the flow result report.</p> <p>In addition, in cross-border flow, one of the following conditions must be met: ① mobile countries have equal personal data protection rules as Indonesia; ② has international consent between Indonesia and mobile countries; contracts between the personal data administrator of the ③ mobile source and the personal data administrator of the mobile destination; and ④ gets the consent of the data subject.</p> <p>2. The Personal Data Protection Act (Draft): Cross-border data flows should reach the level of protection without harming individuals.</p>	<p>I. Electronic Systems and Electronic Transactions, Administrative Decree No.71 of 2019 (Government Regulation No.71 of 2019 on the Administration of Electronic Systems and Transactions) Article 20: Electronic system providers in the public sector are obliged to manage, process, or preserve electronic systems and electronic data in Indonesia. However, as an exception to this obligation, the public electronic system operators can keep the data abroad in Indonesia in the case that the storage technology cannot be used in Indonesia. Whether the benchmark is in the “inaccessible” situation is decided by the committee composed of relevant provincial departments such as the Ministry of Communications and Information, but the benchmark is not made public.</p> <p>2. The Finance Department of Indonesia also requires non-bank financial institutions and commercial banks in Indonesia to undertake the domestic preservation and domestic custody obligations of the data.</p>
Korea	<p>Under the framework of South Korean data protection law, any company or government agency wishing to transfer personal information outside of South Korea is restricted. According to its Personal Information Protection Law, the consent of the data subject must be obtained in advance when providing personal information to overseas third parties. When IT services provide, outsource, or store the personal information of IT service users overseas, they must obtain prior consent of IT service users and implement corresponding safeguard measures.</p>	<p>I. Article 17 of the Personal Data Management Regulations only allows the transfer of personal data to be abroad under temporary circumstances, and the consent of the data subject must be obtained when transferring data to other countries.</p> <p>2. Under presidential Decree No.30892, information technology enterprises without an address or place of business in South Korea must appoint domestic agents in writing to strengthen the protection of personal data.</p>

jointly build a multilateral governance mechanism for cross-border data flow in Asia, which can serve as a model for a global multilateral governance mechanism. Although achieved in Asia, the multilateral governance mechanism of multilateral negotiations is difficult. However, we also aim to see it significantly reduce supervision and compliance costs, making Asian cross-border data governance decisions and execution more transparent and inclusive. This would enable multinational enterprises to form more stable business expectations and a more concise data use and privacy protection policy (Yu, 2004, pp. 323–328). Therefore, we need to analyse the uniqueness of cross-border data flow in Asia by combining the current cross-border data governance routes led by the EU and the US, and accordingly put forward the idea of building a mutual trust platform for cross-border data flow in Asia.

3. The uniqueness of cross-border data flows in Asia and the necessity to build a platform for mutual trust

3.1 Differences between cross-border data flow in Asia and the European Union and the United States

The Asian cross-border data flow mechanism should be based on the integrated development of the Asian region, with its core concept of realising mutual trust and win-win results, and should focus on the unique governance needs and social trust foundation of the Asian region. This is different from the cross-border data flow mechanism and relevant bilateral agreements implemented by the EU and the US, which are based on maximising their own interests.

3.1.1 Differences in the governance demand and governance concepts of cross-border data flow

In the governance of cross-border data flow, the EU tries to achieve the goal of the digital single market through unified rules and leads the global reconstruction of the data protection rule system with high standards of data protection. On the one hand, it aims to unify legislation to eliminate barriers to the free flow of data within the EU. On the other hand, it confirms the cross-border data flow of “white list” countries based on “adequacy protection,” allowing EU data to follow its high standards of data protection while competing for an international voice in cross-border data flow standards (Mattoo and Meltzer, 2018, pp. 769–789). The US maintains its industrial competitive advantage as its main governance demand. First, it relies on its existing dominant position in the digital economy and international trade, incorporating “cross-border data free flow” into various trade negotiations to avoid the trend of fragmentation of the Internet and to prevent strict controls on cross-border data from hindering the overseas expansion of its large Internet enterprises (Selby, 2017, pp. 216–218). Second, it strengthens its dominance by limiting data exports of key technologies and foreign investment in specific data areas. Moreover, it has expanded the effect of “long-arm external jurisdiction” by establishing the data stored on the servers of other countries according to the needs of law enforcement and allowing the government to transfer the data stored on them by multinational companies (Bilgic, 2018, pp. 331–332).

However, even though the EU and the US have different governance ideas on cross-border data flow, both unilateral governance mechanisms use their existing international influence and economic strength to compete for cross-border data flow standards, to formulate a voice, and to seek the benefits of the national digital economy (Baker, 2005, pp. 1322–1325). Such a unilateral governance mechanism imposes the concepts and principles of the rule of law on other national and regional organisations with less influence and weak economic strength, requiring them to establish the same governance mechanism to qualify for cross-border data flows (Danchin, 2007, pp. 47–51). However,

such promotion cannot adapt to other countries' political, economic, cultural, and historical factors and produces relatively strong rejection and resistance; it may even be regarded as institutional imperialism ("institutional imperialism" refers to a scenario where a party with strong economic and political strength in international trade uses its advantage to institutionalise its national interests and incorporate them into the system of national trade rules), thereby asserting hegemony. This is not conducive to mutual trust and win-win situations between countries (Piilola, 2003, p.207). Take the governance of the cross-border flow of personal data as an example. Some countries or regional organisations seek to extend their domestic protection standards for cross-border flow of personal data globally, which has resulted in a conflict of values with other sovereign countries (Yuen, 2007, p.41). Furthermore, a significant number of bilateral governance agreements currently led by the EU and the United States still fail to address the cross-border data flow problem in the Asian region. Although these bilateral governance agreements are cheaper and more operable, their application scope remains too narrow, and they cannot overcome the sovereignty erosion caused by the considerable disparity in national power (Baker, 2005, pp. 1322–1325). Additionally, an excess of bilateral governance agreements among countries in Asia may create a more complex and less transparent cross-border data flow governance mechanism, which is detrimental to the integrated development of the regional digital economy in Asia.

Therefore, the governance model between the EU and the US, along with its leading bilateral governance agreement, is not applicable to addressing the cross-border data flow problem in the Asian region. To promote cross-border data flow in the Asia region and realise the integrated development of the regional digital economy, the establishment of a multilateral governance mechanism would be a more appropriate path. In terms of existing multilateral governance agreements, the Asia-Pacific Economic Cooperation (APEC) "Cross-border Privacy Rules" (CBPR) are more representative and operable, and they also have significant reference and guiding relevance for the construction of a multilateral governance mechanism for cross-border data circulation in Asia. Currently, it is applicable solely to the cross-border flow of personal data by international enterprises and is a voluntary standard. It relies on internal management (such as articles of association, reward and punishment mechanisms, contracts, etc.) as the main means of security guarantee and employs legal sanctions as the final safeguard measures. It was created as a platform to balance the disparities in the level of protection of the cross-border flow of personal data across different countries.

As a multilateral governance agreement issued by APEC, the CBPR exhibits notable differences from the multilateral governance agreement issued by the Organization for Economic Cooperation and Development (OECD), and these differences underscore the particularity of the governance concept of cross-border data flow in Asia. First of all, the OECD member countries have little difference in economic strength, as they are all industrialised countries with strong economic capabilities; therefore, they do not face the uneven mutual trust problem regarding data security protection levels. In contrast, the CBPR constraints faced by APEC members have greater differences in economic strength and data security protection levels, leading to significant variations in the governance concept of cross-border data flow. For instance, Japan and South Korea have adopted comprehensive unified legislation for cross-border personal data flow, while India focuses on personal data localisation processing, and Indonesia has yet to promulgate a personal data protection law, among others. In regions where such levels of protection are quite different and governance ideas vary, cross-border data flows require a higher demand for mutual trust among countries. Secondly, the entry threshold of the OECD results in a more compact organisational structure, making it easier for member states to understand the concept of the rule of law. Therefore, the multilateral governance agreement issued by the OECD is less transparent and open.

However, APEC's zero-entry threshold requirements and looser organisational structure lead to a need for more open and transparent consultation mechanisms (Zhang, 2018, pp. 37–48). Moreover, compared with the OECD, APEC member states exhibit greater diversity in language, culture, politics, and social governance concepts, making it more difficult for APEC to coordinate with its governments to form a consensus and a mandatory multilateral governance mechanism. These three issues are also the unique challenges that Asia must face in building a multilateral governance mechanism for cross-border data flow compared with other regions.

3.1.2 Differences in the trust basis of cross-border data flows

In addition to the differences in the governance concepts of cross-border data flows, the cross-border data flows in Asia are also different from those in the EU and the US in the way that trust is built. Cross-border data flows are bound to face the problem of how to build trust between multinational governments, enterprises, and users. The idea of the EU is to establish a complete personal data rights system and high-standard cross-border data flow rules in order to reshape the trust of the three in cross-border data flow with institutional trust. The United States, on the other hand, uses the market to reshape trust, giving companies more autonomy for cross-border data flows, and ensuring trust between users and businesses through mandatory disclosure and supervision by the Federal Trade Commission (Farrell and Newman, 2019, pp. 1–52). Therefore, in the EU's cross-border data flow governance mechanism, the decision-making of the legislature and the enforcement of the judiciary play a greater role in trust-building. In the cross-border data flow governance mechanism in the US, trust-building depends more on enterprise decision-making and technological solutions (Brownsword and Yeung, 2008, pp. 263–268).

However, Asia's unique politics, religion, and culture will make the foundational building of its social trust different from that of the West (Mishler and Rose, 2001, pp. 30–62). First, according to empirical studies, public trust in government is significantly higher in Asian countries than in Western countries (Inoguchi, 2017, pp. 143–145). This means that the mutual trust-building of cross-border data flows in Asia depends more on the promotion and communication between government agencies. Second, in Asian countries, the main factor determining the level of social trust in government is policy performance, where the credibility of a government agency depends largely on the extent of the desired economic outcomes (Wang, 2005, pp. 155–171). In terms of cross-border data flow, this is reflected in the fact that the mutual trust basis of cross-border data flow in Asia is the expected result of stabilising users and enterprises by cooperating with national governments. Finally, although Asia has its own unique social information base, according to empirical research, social trust in Asia also needs to be interpreted and constructed from the perspective of the legal system, just like in the West, rather than being determined by culture. The public's trust in government institutions arises from the rational response and predictability of individuals to the laws and regulations issued by government agencies (North, 1990, pp. 1–33). People with different cultural orientations may respond differently to similar laws and regulations, but this does not mean that culture can deny the influence of laws and regulations on trust construction. Therefore, even if Asia has a diversity of cultural backgrounds, we should not give up building the trust of Asian cross-border data flow from the perspective of laws and regulations; after all, the public and enterprise trust in Asian cross-border data flow depends on whether the Asian governments have the ability to provide a set of good governance mechanisms for the public and enterprises, rather than on whether countries have the same cultural background.

3.2 The significance and goals of building the Asian Cross-Border Data Flow Mutual Trust Platform

In dealing with governing cross-border data flows, both China and Japan have unanimously stressed the importance of “trust mechanism” building. In China’s cross-border data flow governance mechanism, ensuring data security to achieve a credible free flow of data is a governance policy for China to reshape the mutual trust among governments, enterprises, and users (Xu, 2021, pp. 22–37). The Japanese government has clearly put forward the “Data Free Flow with Trust (DFFT),” a free data flow target based on “trust,” which seeks to promote mutual trust through the sharing of values, the rule of law concept, and the consensus of the cross-border data circulation governance mechanism. It has embodied the DFFT concept in its signed multilateral agreements, such as bilateral agreements, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), and the Regional Comprehensive Economic Partnership Agreement (RCEP). Through e-commerce negotiations with the World Trade Organization (WTO), Japan’s co-speaker further expands the concept of DFFT.

Therefore, with mutual trust as the core principle and based on the technological innovation and organisational concept of the Internet platform, the construction of a mutual trust platform guaranteed by legal procedures will be a feasible path to realise the multilateral governance mechanism of cross-border data flow in Asia. This mutual trust platform for cross-border data flow will achieve the goal of democratic, prosperous, and stable cross-border data flow governance in Asia through the shape of trust.

First, the high level of trust between the Asian public, businesses, and governments helps to ensure democracy and inclusiveness in multilateral governance mechanisms. The trust platform is built to facilitate governments, enterprises, and users to participate in the governance of cross-border data flow. They can obtain relevant information, communicate, and participate in various governance processes on the trust platform. At this point, the mutual trust created by the mutual trust platform will become a kind of social capital, and the stakeholders who promote the cross-border data flow can interact and communicate more inclusively and efficiently (Putnam, Leonardi, and Nonetti, 1993, pp. 1–52). In addition, the emergence of such social capital is conducive to integrating countries into a region and enhancing the identity of Asian countries to the concept of regional integration development in Asia.

Second, the high level of trust shaped by the mutual trust platform helps to maintain the prosperity of cross-border trade in Asia. In a low-trust environment, it is difficult for companies to innovate and pursue business transactions. Only the continued prosperity of the Asian digital economy can be achieved when trust permeates Asian society (Fukuyama, 1995, pp. 1–23). The construction of the mutual trust platform can not only greatly reduce the compliance cost of Asian multinational enterprises in cross-border data flow but also promote business cooperation and transactions between enterprises, which can effectively solve the sustainable dilemma faced by the current regional integration development in Asia.

Finally, the mutual trust platform plays a key role in reducing the governance complexity of cross-border data flows and ensuring the stability of cross-border data flows. In an environment lacking trust, countries will have to continuously evaluate the flow and use of data for future predictability, and such continuous security assessment amidst mutual distrust will greatly increase the complexity of cross-border data flow governance. Social trust, which also encourages countries with different governance theories in Asia to follow some common minimum rules, also warns powerful subjects not to act against basic morals.

Therefore, in order to promote the cross-border data flow in Asia and realise the regional integrated development of the digital economy in Asia, it is particularly

important for the construction of the mutual trust platform. With high trust, data flows are more certain, faster, and less costly, and the digital economy prospers in Asia. If trust is too low, data flows are more uncertain, slower, and more costly, making it difficult for Asia to integrate across regions with digital technology.

4. Digital technology, organisational model, and legal procedures for building an Asian Cross-Border Data Flow Mutual Trust Platform

The construction of a mutual trust platform for ensuring the democracy, prosperity, and stability of cross-border data flow governance in Asia needs to be jointly promoted from three dimensions: digital technology, organisational model, and legal procedures.

4.1 Technical basis of the Asian Cross-Border Data Flow Mutual Trust Platform

Technical experts provide a technical solution based on blockchain and cloud computing technology on how to use digital technology to build a mutual trust platform for cross-border data flow governance (see Chart 1). The digital technology architecture builds a global cloud in security gateways in several different countries. When the application of a multinational enterprise needs to access data from a specific country, the global cloud can collect and store data from the country's data centres through the country's security gateway. In the process of collection and storage, the blockchain records the flow of data. When the enterprise application reports any improper data flow behaviour to the platform, the global cloud verifies the authenticity of the report by auditing the blockchain, punishes the security gateway that caused the misconduct even if the report is true, and punishes the application of the enterprise even if the report is false (Rahman et al., 2020, pp. 1476–1486). In this digital technology architecture, technical experts can

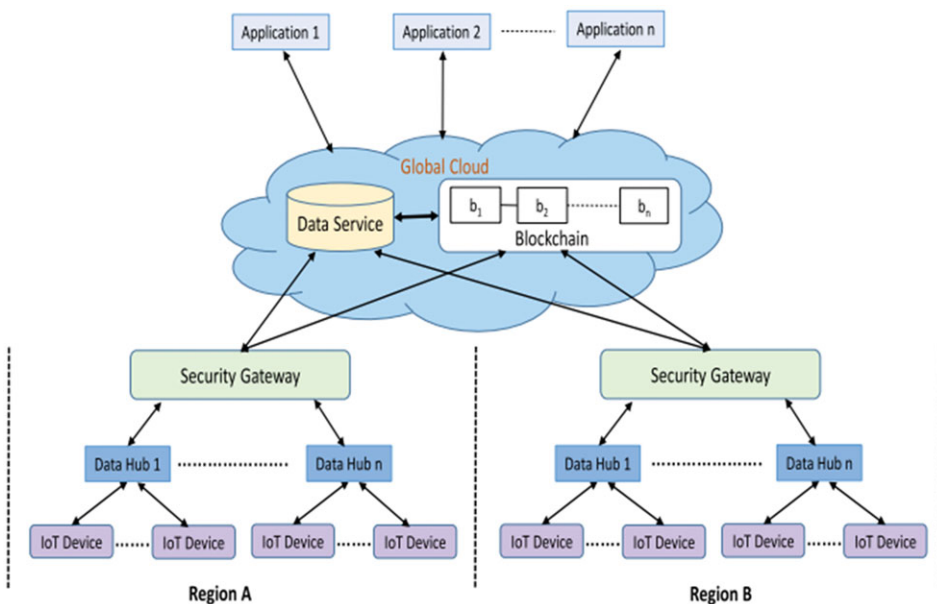


Chart 1. Double-loop System of Risk Decision-making in China. Sources: Mohammad Shahriar Rahman, Abdullah Al Omar, Md Zakirul Alam Bhuiyan, et al. (2020). 'Accountable Cross-Border Data Sharing Using Blockchain under Relaxed Trust Assumption', *IEEE Transactions on Engineering Management*, 67(4), p.1479.

obtain correct and complete information on cross-border data flow, ensuring that governments and enterprises in multiple countries, by designing five algorithms for data access requests, cross-border data flow, blockchain transactions, and improper behaviour detection, can operate effectively. It is also based on the use of blockchain technology that the platform can guarantee the authenticity of data flow information in the multilateral governance mechanisms, eliminating the possibility of the government and enterprises making misstatements about cross-border data flow governance, thus shaping trust between governments and enterprises in various countries.

4.2 Organisational mode of the Asian Cross-Border Data Flow Mutual Trust Platform

“Platform” is not only a form of digital technology but also a new organisational model rooted in digital technology. Through the digitisation and large-scale processing of information, it eliminates the pipeline gatekeeper in the traditional information flow and creates a community feedback loop accordingly. While “governance” is proposed in relation to the unilateral management mode, its purpose is to construct a cooperative network that encourages multiple subjects to make behavioural decisions together (Bevir, 2011, pp. 1–16). Therefore, from the perspective of organisational models, Asian cross-border data flow governance based on a mutual trust platform can be understood as a cooperative network with multiple subjects in Asia founded on Internet-platform technology, which jointly makes cross-border data decisions through a community feedback loop.

From this perspective, the “government” responsible for promoting and coordinating the governance of cross-border data flow is also used as a “platform.” These scholars who advocate that “government is a platform” believe that government is also essentially a model of collective organisation. In the traditional organisational model, the administration is the “pipeline” connecting the sender and receiver of cross-border data flow, which can be replaced by the “platform.” Therefore, when transferring “pipeline” government into “platform”-type government through digital technology, we need decentralised measures to stimulate enterprise innovation in building platforms, and the government needs to build the foundation of the initial core system and participation rules; let others focus on its application expansion, namely, “platform government means the government will be reduced to the most basic part” (O’Reilly, 2011, pp. 13–40). To pursue an organisational mechanism with less control, but more interaction, grid, and collaboration, shaping a social governance model centred on the government platform and allowing others to participate in an orderly manner” (Janssen and Estevez, 2013, pp. 1–8). Therefore, the concept of a mutual trust platform in the cross-border data flow governance in Asia is not only a utilisation of digital technology but also a penetration process of the platform organisation mode into the traditional cross-border data flow governance model (Nieborg and Poell, 2018, pp. 4275–4292).

Under the organisational model of the platform, the roles of government, enterprises, and the public in cross-border data governance in Asia would evolve. The government is no longer the maker of the rules for cross-border data flow, but rather the manager responsible for coordinating and unifying multiple opinions and proposals. Instead of formulating specific codes of conduct in great detail, the government designs incentives to encourage enterprises and the public to actively participate in the governance process of cross-border data circulation. Enterprises no longer passively abide by established rules, but become the rule designers and architecture builders of cross-border data flow governance through the platform. They consistently leverage market capital and technological innovation to develop a more secure and efficient governance architecture for cross-border data circulation, thereby improving the rule system and code architecture on the platform. The public is no longer a vulnerable group that can only rely on the

government; they can actively evaluate cross-border data circulation behaviour through the platform and provide feedback to the government and enterprises concerning the existing rules and governance architecture. Consequently, how to effectively coordinate among the governments, enterprises, and the public of Asian countries to make joint decisions becomes a significant challenge, which necessitates resolution through the legal process.

4.3 Legal guarantee of the Asian Cross-Border Data Flow Mutual Trust Platform

It can be observed from the preceding discussion that, as a multilateral governance mechanism, the mutual trust platform for Asian governments, enterprises, and the public to jointly govern cross-border data flow cannot avoid the communication and consultation of multiple subjects. The values, power structures, and mutual relations of these subjects will inevitably differ. Finding a unified order of cross-border data flow amid these multiple factors that contribute to chaos is a complex problem that the Asian Cross-Border Data Flow Mutual Trust Platform must confront. The legal process, which focuses on the communication between multiple subjects, serves as a necessary medium to eliminate this complexity. It can systematically filter the information in the communication process, simplify interactions between multiple agents, and transform the chaos on the mutual trust platform into order. Consequently, a fair legal procedure represents the ideal condition or evaluation standard for multiple subjects to communicate regarding cross-border data flow governance matters, and the adequacy and effectiveness of multi-subject communication require a fair legal procedure to guarantee them. Specifically, the legal procedures to underpin the Asian Cross-Border Data Flow Circulation Mutual Trust Platform should establish corresponding collaborative behaviour rules around the division of governance roles outlined earlier.

First of all, in the decentralised governance platform of blockchain, the Asian governments that act as platform managers need to jointly build the initial and core basic system and participation rules, and encourage enterprises and the public to participate in the application extension and improvement of the governance platform. Thus, in addition to the cross-border data flow multilateral agreement between Asian governments, government laws also need to stipulate the corresponding enterprise participation procedures and public participation procedures, such as corporate governance, cross-border data flow mechanism evaluation and access programme, rules for enterprises to provide annual reports to the government or governance platform, specific public disclosure obligations for enterprises in cross-border data flow, etc.

Second, as the specific rule-makers and network architecture builders of mutual trust platforms for cross-border data flow, Asian companies need to incorporate their commercial management mechanisms into the formal governance mechanisms through due process. On the one hand, we need to set up the corresponding corporate responsibility system, which pursues interest maximisation, into the cross-border data flow governance demands of public decision-making in order to provide a legitimate basis for the participation of enterprises in cross-border data flow governance; for example, the law needs to establish enterprise control over cross-border illegal exemptions in the data flow process. On the other hand, the law should interpret the private compromise, agreement, and consensus on the Asian Cross-Border Data Flow Mutual Trust Platform through legal language, making it comparable and communicative, so as to transform the contractual relationship between commercial enterprises into abstract social consensus. For example, the law can translate the typical commercial consensus on cross-border data flow among Asian companies into legal norms by establishing standard contracts for cross-border data flow. In addition, the law can establish corresponding algorithm authentication procedures to incorporate the

code architecture used in business practice, ensuring the security of cross-border data flow within the Asian Cross-Border Data Flow Trust Platform.

Moreover, in order to ensure effective public participation in the construction of the Asian Cross-Border Data Flow Mutual Trust Platform, the legal procedure should include the following four aspects. First, the law should stipulate the obligation of interpretation and reasoning regarding the algorithmic use of the mutual trust platform, so as to break the information asymmetry between the public, the government, and enterprises, and to protect citizens' rights to know and to participate in governance. This includes that the government and enterprises have a legal obligation to explain the algorithmic operation principles of the mutual trust platform to the public through special texts and text examples, and they have the obligation to significantly publicise any changes to the algorithm of the mutual trust platform. Second, in order to ensure that the public and the government can make informed decisions on cross-border data flows, the law should provide individuals with choice through informed consent rules. This informed consent rule should not only be stipulated in the law, but also be embedded in the code architecture of the trust platform. Third, the law needs to ensure public supervision channels. The public has the right to obtain relevant information through the mutual trust platform and to publicly express relevant opinions and suggestions on the cross-border data flows that have been sent. Fourth, the law also needs to provide for individual relief procedures for cross-border data flows. When the government or enterprises commit illegal acts, individuals should have channels for appeal and relief, and be able to file relevant lawsuits and seek accountability in accordance with legal procedures.

5. Conclusion

After the huge damage to the Asian economy caused by the novel coronavirus, the digital transformation of society has become a major opportunity for Asian economic recovery and regional integrated development. However, to ensure their own network and data security, Asian countries have introduced very different laws and regulations on cross-border data flow. The differences in governance theories and the uncertainty in governance standards caused by these laws and regulations have seriously hindered the free flow of cross-border data in Asia, further obstructing the regional integrated development of Asia's digital economy. The current unilateral governance mechanism and bilateral governance agreements guided by the EU and the US cannot solve the specific problems in cross-border data flow in Asia, further increasing the complexity of governance conflicts. Regarding special issues such as the large economic strength gap, loose organisation, and cultural diversity among Asian countries, it is urgent to build a multilateral governance mechanism with trust as the core. This means establishing a cross-border data flow mutual trust platform in Asia, with mutual trust as the core principle and democratic, prosperous, and stable cross-border data circulation and governance as the goal.

The construction of the Asian Cross-Border Data Flow Mutual Trust Platform must commence from three perspectives: digital technology, organisational model, and legal process. From the perspective of digital technology, the Asian Cross-Border Data Flow Mutual Trust Platform comprises a set of digital technology architectures based on blockchain and cloud computing that aim to realise decentralised governance and ensure the authenticity and reliability of cross-border data flow information. From the perspective of the organisational model, cross-border data flow governance in Asia, based on the mutual trust platform, can be understood as a cooperative network of multiple stakeholders in Asia that collectively make cross-border data decisions through a community feedback loop. Within this cooperative network, the government serves as the

platform manager for coordination, unification, and incentive supervision; enterprises act as the designers of specific rules and network code; and the public functions as the evaluator through full participation and positive feedback. The legal process necessitates the integration of Asian governments, enterprises, and the public into the cooperation network. As a crucial medium to eliminate the complexity of this cooperative network, it will transform the chaos inherent in the mutual trust platform of Asia through the directional screening of information during communication and by simplifying the interactions of Asian cross-border data flow into an ordered system. Therefore, the power structure and mutual relationships among multiple stakeholders can operate freely and coordinate through legal procedures within the Asian Cross-Border Data Flow Mutual Trust Platform.

References

- Anupam, C. and Le, U. P. (2015). 'Data nationalism', *Emory Law Journal*, 64(3), pp. 679–704.
- Asian Development Bank. (2021). *Asian Economic Integration Report 2021: Enabling Digital Platforms in Asia and the Pacific*. Available at: <https://www.adb.org/publications/asian-economic-integration-report-2021> (Accessed: 10 October 2024).
- Baker, M. B. (2005). 'No country left behind: The exporting of U.S. legal norms under the guise of economic integration', *Emory International Law Review*, 19(3), pp. 1322–1380.
- Bevir, M. (2011). 'Governance as theory, practice, and dilemma', in Bevir, M. (ed.) *The SAGE handbook of governance*. California: SAGE Publications Ltd, pp. 1–16.
- Bilgic, S. (2018). 'Something old, something new, and something moot: The privacy crisis under the CLOUD Act', *Harvard Journal of Law & Technology*, 32(1), pp. 331–332.
- Brownsword, R. and Yeung, K. (eds.) (2008). *Regulating technologies: Legal futures, regulatory frames and technological fixes*. London: Hart Publishing, pp. 263–268.
- Cate, F. H. (1999). 'The changing face of privacy protection in the European Union and the United States', *Indiana Law Review*, 33(1), pp. 173–176.
- Dai, Y. (2021). *Cross-border data transfers regulations in the context of international trade law: A PRC perspective*. Singapore: Springer, pp. 119–138.
- Danchin, P. G. (2007). 'U.S. unilateralism and the international protection of religious freedom: The multilateral alternative', *Columbia Journal of Transnational Law*, 40, pp. 47–51.
- Farrell, H. and Newman, A. L. (2019). *Of privacy and power: The transatlantic struggle over freedom and security*. New Jersey: Princeton University Press, pp. 1–52.
- Fukuyama, F. (1995). *Trust: Social virtues and creation of prosperity*. New York: Free Press, pp. 1–23.
- Gao, H. (2018). 'Digital or trade? The contrasting approaches of China and US to digital trade', *Journal of International Economic Law*, 21(2), pp. 297–321.
- Hu, W. and Kong, H. (2019). 'Yindu shuju bendihua yu kuajing liudong lifa shijian yanjiu [Indian data localization and cross-border flow legislation practice]', *Jisuanji Yingyong yu Ruanjian [Computer Applications and Software]*, 36(8), pp. 306–310.
- Inoguchi, T. (2017). 'Confidence in institutions', in Inoguchi, T. and Tokuda, Y. (eds.) *Trust with Asian characteristics: Interpersonal and institutional*. Singapore: Springer, pp. 143–167.
- Janssen, M. and Estevez, E. (2013). 'Lean government and platform based governance—doing more with less', *Government Information Quarterly*, 30(1), pp. 1–8.
- Mattoo, A. and Meltzer, J. P. (2018). 'International data flows and privacy: The conflict and its resolution', *Journal of International Economic Law*, 21(4), pp. 769–789.
- McDonald, A. M. and Cranor, L. F. (2008). 'The cost of reading privacy policies', *A Journal of Law and Policy for the Information Society*, 4, pp. 543–568.
- Mishler, W. and Rose, R. (2001). 'What are the origins of political trust? Testing institutional and cultural theories in post-communist societies', *Comparative Political Studies*, 34(1), pp. 30–62.
- Nieborg, D. B. and Poell, T. (2018). 'The platformization of cultural production: Theorizing the contingent cultural commodity', *New Media & Society*, 20(11), pp. 4275–4292.
- North, D. C. (1990). *Institutions, institutional change and economic performance*. New York: Cambridge University Press, pp. 1–70.
- O'Reilly, T. (2011). 'Government as a platform', *Innovations Technology Governance Globalization*, 6(1), pp. 13–40.
- Piilola, Anu (2003). 'Assessing theories of global governance: A case study of international antitrust regulation', *Stanford Journal of International Law*, 39, pp. 207–213.

- Putnam, R. D., Leonardi, R., and Nonetti, R. Y. (1993). *Making democracy work: Civic traditions in modern Italy*, new edition. Princeton: Princeton University Press, pp. 1–82.
- Rahman, M. S., Omar, A. A. I., Bhuiyan, M. Z. A., Basu, A., Kiyomoto, S., and Wang, G. (2020). 'Accountable cross-border data sharing using blockchain under relaxed trust assumption', *IEEE Transactions on Engineering Management*, 67(4), pp. 1476–1486.
- Selby, J. (2017). 'Data localization law: Trade barriers or legitimate responses to cybersecurity risk, or both?', *International Journal of Law and Information Technology*, 25(3), pp. 216–218.
- Wang, Z. (2005). 'Before the emergence of critical citizens: Economic development and political trust in China', *International Review of Sociology*, 15(1), pp. 155–171.
- Xu, D. (2020). 'Lun kuajing shuju liudong guizhi qiye shuangxiang hegui de fazhi baozhang [Legal guarantee for two-way compliance of enterprises subject to regulation of cross-border data flow]', *Dongfang Faxue [Oriental Law]*, 74(2), pp. 185–197.
- Xu, K. (2021). 'Ziyou yu anquan: shuju kuajing liudong de zhongguo fangan [Freedom and security: The China plan for cross-border data flow]', *Huanqiu Falu Pinglun [Global Law Review]*, 43(1), pp. 22–37.
- Yu, P. K. (2004). 'Currents and crosscurrents in the international intellectual property regime', *Loyola of Los Angeles Law Review*, 38(1), pp. 323–328.
- Yuen, S. (2007). 'Exporting trust with data: Audited self-regulation as a solution to cross-border data transfer protection concerns in the offshore outsourcing industry', *Columbia Science and Technology Law Review*, 9(2), pp. 41–45.
- Zhang, J. (2018). 'Geren shuju kuajing chuanshu xianzhi jiqi jie jue fangan [Cross-border transmission of personal data in a big data era: Limits and solutions]', *Dongfang Faxue [Oriental Law]*, 66(6), pp. 37–48.