Frontiers of Law in China
-Selected Publications from Chinese Universities
Vol. 17, No. 3 September 2022 412–439
DOI 10.3868/s050-011-022-0040-7

Towards a Global Regulatory Framework for Cross-Border Data Flows —Fundamental Concerns and the China's Approach

LIU Jinrui

Abstract Cross-border data flows not only involve cross-border trade issues, but also severely challenge personal information protection, national data security, and the jurisdiction of justice and enforcement. As the current digital trade negotiations could not accommodate these challenges, China has initiated the concept of secure cross-border data flow and has launched a dual-track multi-level regulatory system, including control system for overseas transfer of important data, system of cross-border provision of personal information, and system of cross-border data request for justice and enforcement. To explore a global regulatory framework for cross-border data flows, legitimate and controllable cross-border data flows should be promoted, supervision should be categorized based on risk concerned, and the rule of law should be coordinated at home and abroad to promote system compatibility. To this end, the key is to build a compatible regulatory framework, which includes clarifying the scope of important data to define the "Negative List" for preventing national security risks, improving the cross-border accountability for protecting personal information rights and interests to ease pre-supervision pressure, and focusing on data access rights instead of data localization for upholding the jurisdiction of justice and enforcement.

Keywords cross-border data flows, personal information, important data, national security, jurisdiction of justice and enforcement, global regulatory framework

I. Concerns and Differences on Regulation Regarding Cross-Border Data Flows Worldwide 415
A. Protection of Personal Information Rights and Interests 416
B. Safeguards against National Security Risks 418
C. Jurisdiction Requirements for Justice and Enforcement 421
D. Face up the Common Legitimate Concerns 423
II. China's Exploration of Promotion and Control of Cross-Border Data Flows 424
A. The Concept of Secure Cross-Border Data Flow 425

Translated from 行政法学研究 (*Administrative Law Review*), 2022 (4): 73–88.

LIU Jinrui 刘金瑞 (✉)
The Institute of Rule of Law, China Law Society, Beijing 100081, China
E-mail: jinruiliu1987@163.com

1. Paying Equal Attention to Effective Protection and Legal Utilization 425
2. Coordinate Domestic Rule of Law and Foreign-Related Rule of Law 426
B. The Dual-Track Multi-Layer Regulatory System 427
1. Control System for Overseas Transfer of Important Data to Safeguard National Security 427
2. System of Cross-Border Provision of Personal Information for Protection of Personal Rights and Interests 428
3. System of Cross-Border Data Request for Justice and Enforcement under the Sovereign Jurisdiction 429
C. China's Continuing Exploration of Cross-Border Data Flow Management 430
III. China's Approach Regarding Exploration of a Global Regulatory Framework for Cross-Border Data Flows 431
A. The Basic Philosophy of Global Regulatory Framework for Cross-Border Data Flows 431
1. Promotion of Legitimate and Controllable Cross-Border Data Flow 432
2. Categorized Supervision Based on Risk Concerns 432
3. Coordinate the Rule of Law at Home and Abroad to Promote System Compatibility 433
B. Exploration of Compatible Framework of Global Regulatory Framework for Cross-Border Data Flows 434
1. Prevention of National Security Risks: Clarification of the Scope of Important Data to Define the "Negative List" 435
2. Protecting Personal Information Rights and Interests: Improvement of the Cross-Border Accountability to Ease the Pre-Supervision Pressure 436
3. Upholding Justice and Enforcement Jurisdiction: Focusing on Data Access Rights Instead of Relying on Data Localization 438

Cross-border data flow generally refers to data transmission between servers located in different jurisdictions.[1] This cross-border nature has made its governance a global issue from the very beginning. The discussion on this issue began in the 1970s and focused on personal information and privacy protection.[2] The characteristic achievements were Council Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of the Organization for Economic Cooperation and Development (OECD) in 1980 and the Convention on Personal Protection in

[1] See Business Software Alliance, "Cross-Border Data Flows, Business Software Alliance," BSA (November 2017), available at https://www.bsa.org/policy-filings/cross-border-data-flows (last visited Jan. 25, 2022).

[2] Personal information and privacy are viewed different in legal domains, yet they are considered equal to each other in the digital trade negotiations.

Automatic Processing of Personal Data of the European Council in 1981.[3] In the era of the digital economy, digitalization has driven a new round of economic globalization, and cross-border data flows and digital trade have increased substantially, becoming a new engine for global economic growth. Studies have shown that cross-border data flows contributed 2.8 trillion US dollars to world economic growth in 2014, and this figure is expected to reach 11 trillion US dollars in 2025.[4] Thus, the discussion of cross-border data flows has gradually shifted to e-commerce and digital trade.[5]

In February 2016, the Trans-Pacific Partnership Agreement (TPP) was signed, becoming the first trade agreement containing binding rules for cross-border data flows. After the US withdrew from this agreement in 2017, this agreement was renamed the Comprehensive and Progressive Trans-Pacific Partnership Agreement (CPTPP).[6] After one-year-plus of discussions, 76 members of the World Trade Organization (WTO), including China, formally signed the Joint Statement on E-Commerce in January 2019, and jointly initiated plurilateral negotiations on e-commerce, in which cross-border data flow was one of the key topics. In addition, regional or bilateral trade agreements began to regulate cross-border data flow and some agreements, such as the Digital Economy Partnership Agreement (DEPA) signed by Singapore, New Zealand, and Chile in 2020, fundamentally referenced CPTPP.

In fact, cross-border data flow is not only related to economic issues such as cross-border trade, but also related to non-economic concerns such as personal rights protection, national security, and sovereign jurisdiction. Now, countries hold a range of different interpretations and claims on these issues, and trade agreements emphasizing the economic dimension can not undertake the task consensus-building, which results in not only the failure to conclude trade agreements, but also increasingly "fragmenting" global digital governance. Thus, cross-border data flow, if not properly addressed, has the potential to slow down the globalization of the digital economy, infringe upon personal rights and interests, damage social welfare, and exacerbate zero-sum games between countries. In this context, exploring global regulation system of cross-border data flows has become one of the major challenges for global governance.

From the perspective of global regulation theory, the formation of such global

---

[3] OECD, Council Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD Doc. C (80) (58) final. Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, E. T. S. 108, 28. I. 1981.

[4] McKinsey Global Institute, *Digital Globalization: The New Era of Global Flows*, at 10 (Mar. 2016), available at https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows (last visited Jan. 25, 2022).

[5] See Merit E. Janow & Petros C. Mavroidis, "Digital Trade, E-Commerce, the WTO and Regional Frameworks," 18 *World Trade Review*, S1–S (2019).

[6] As far as cross-border data flow is concerned, CPTPP provisions are completely consistent with TPP provisions.

regulation system needs the participation of governments, international organizations and enterprises. It is necessary to introduce procedural rules to ensure transparency, participation and reasonable decision-making from the perspective of "global administrative law." [7] It is also necessary to build an institutional framework to promote the compatibility of substantive rules of different countries. This paper focuses on exploring the compatible institutional framework, sorts out the fundamental concerns and main differences in global regulations on cross-border data flows, and develops China's domestic systems to present the "China Approach" for global regulation of cross-border data flows.

I. Concerns and Differences on Regulation Regarding Cross-Border Data Flows Worldwide

At present, the governance of cross-border data flow has not been listed as an individual global topic. Instead, it is still discussed as part of digital trade negotiations. However, according to the definition of OECD, WTO, and the International Monetary Fund, digital trade refers to "all trades that is digitally ordered and/or digitally delivered." [8] Clearly, digital trade does not cover cross-border flow of data unrelated to a specific commodity or service transaction, indicating that regulating cross-border data flow should not touch upon trade rules only, and that such regulation should start with the data flow itself. Data can include a wide range of information on economic and social life. Therefore, cross-border data flow involves not only personal information, but also business data, public data, and even data related to national security, which makes it not only economically relevant in association with economic aspect of trade promotion, but also brings a series of non-economic challenges.

In response to these challenges, the legitimate concerns of major economies in regulating cross-border data flows primarily include three aspects: protection of personal information rights and interests, safeguards against national security risks, and jurisdiction requirements for justice and enforcement. To sort out these different concerns and claims from the global perspective, it is necessary to analyze the recent digital trade negotiations and review the legislations in major economies. At the end of 2020, plurilateral negotiations on WTO e-commerce made significant progress and consolidated the negotiating text (hereinafter referred to as "WTO negotiating text").[9] The cross-border data flow primarily involves Article

---

[7] See Benedict Kingsbury, Nico Clichy & Richard B. Steward, 全球行政法的产生 (上) (The Emergence of Global Administrative Law [Part I]), translated by FAN Yunpeng & BI Xiaoqing, 5 环球法律评论 (*Global Law Review*), 124 (2008).

[8] OECD, WTO, & IMF, *Handbook on Measuring Digital Trade*, Version 1, p. 20, available at https://www.oecd.org/sdd/its/handbook-on-measuring-digital-trade.htm (last visited Jan. 25, 2022).

[9] The Consolidated negotiating text is published online, and members' textual proposals are indicated. WTO, *Electronic Commerce Negotiations-Consolidated negotiating text-December 2020*, INF /ECOM/62 /Rev. 1, Bilaterals (Dec. 14, 2020), available at https://www. bilaterals. org /IMG/pdf /wto plurilateral _ ecommerce_draft_consolidated_text. pdf (last visited Jan. 25, 2022).

B.2 "Information Flow" and Article C.2 "Privacy," which are important bases for analyzing the claims of different economies. Due to the limitation of space, the following analyses just touch upon the different claims of the EU and the US.

A. Protection of Personal Information Rights and Interests

Protection of personal information was the earliest concern for regulating cross-border data flows, and it is still a concern today.[10] The EU has developed the most comprehensive legislation on protection of personal information and has comprehensively discussed how to best promote trade through cross-border data flows without damaging the protection of personal data.[11] In 2018, the European Commission adopted the *EU Proposal for Provisions on Cross-border Data Flows and Protection of Personal Data and Privacy*,[12] which was fully consistent with the EU's claims in WTO negotiating text, and primarily included: all parties recognize that protection of personal data and privacy is a fundamental right, and "high standards in this regard contribute to trust in the digital economy and to the development of trade;" each Party may adopt and maintain the safeguards it deems appropriate to ensure the protection of personal data and privacy, "including through the adoption and application of rules for the cross-border transfer of personal data;" each Party should emphasize that "nothing in this agreement shall affect the protection of personal data and privacy afforded by the Parties' respective safeguards." [13]

The EU' s claim is related to its long-standing view that personal data protection should be a fundamental right and strict high-standard protection should be applied. The EU holds that the EU personal data can only be approved to flow to countries or regions with the same level of personal data protection, and cannot be approved to flow to "lower" countries or regions whose level of personal data protection is lower than that of the EU.[14] Article 25 of Directive 95 /46 /EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, adopted by the EU in 1995, stipulated that personal data can only flow to countries that the EU deems

---

[10] Many research literature on the "cross-border flow of data" refers to the cross-border flow of personal data or personal information. See Christopher Kuner, *Transborder Data Flows and Data Privacy Law*, Oxford University Press (Oxford), (2013).

[11] In this paper, "personal information" and "personal data" are not distinguished, and definitions of those quotes follow their source articles.

[12] EU proposal for provisions on cross-border data flows and protection of personal data and privacy, available at https://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157130.pdf (last visited Jan. 25, 2022).

[13] See WTO, *Electronic Commerce Negotiations—Consolidated Negotiating Text*, C. 2. Privacy, Para. 3 Alt. 2, Para. 4 Alt. 2.

[14] Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, *Official Journal of the European Communities*, L 281, 23. 11. 95, pp. 31–50.

to provide "adequate level of protection." [15] Article 45 of the EU General Data Protection Regulation (GDPR) implemented in 2018 maintained this provision. Up to now, only 14 countries or regions have been granted the EU' s "adequacy decision." [16] According to GDPR, there are only two ways to transfer personal data from EU countries to countries or regions that have not been granted the "adequacy decision." First, the data controller or processor can provide "appropriate safeguards," including the binding corporate rules (BCR) allowing intra-corporate transfer, the standard contractual clauses (SCC) approved by the European Commission for inter-corporate transfer and the certification mechanism approved by the EU, etc. Second, the data controller or processor shall comply with statutory derogations, including the explicit consent of the data subject after having been informed of the possible risks, the necessity of data transfer for the performance of the contract, and the protection of important public interests.[17]

Judging from the WTO negotiating text, one can see that the US proposal is somewhat based on the provisions of Article 14. 8 "Personal Information Protection" of CPTPP, which was formulated and adopted under the US leadership. However, there is still a big difference between the WTO and CPTPP versions: The proposal no longer recognizes the first paragraph of this Article; instead, it suggests that "the Parties recognise the importance of ensuring compliance with measures to protect personal information and ensuring that any restrictions on cross-border flows of personal information are necessary and proportionate to the risks presented." The proposal reiterates that the existing personal information protection framework of all parties should be respected, and that each Party shall adopt or maintain measures to protect users' personal information, such as a comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy; each Party should publish information on the protection of users' personal information; the Parties adopting different legal approaches to the protection of personal information should encourage the development of mechanisms to promote compatibility between these different regimes.[18]

The US claim stems from its free market values. It does not regard personal information (privacy) as a fundamental right, but only includes it in the category of

---

[15] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *Official Journal of the European Union*, L 119, 4. 5. 2016, pp. 1–88.

[16] Include Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom and Uruguay.

[17] See General Data Protection Regulation, Art. 46, Art. 47, Art. 49.

[18] See WTO, *Electronic Commerce Negotiations—Consolidated Negotiating Text*, C. 2. Privacy, Para. 3 Alt. 3, Para. 4 Alt. 1, Para. 6, Para. 9, and Para. 10. See CPTPP Art. 14. 8, Para. 1, Para. 2, Para. 4, and Para. 5.

consumer protection in the market economy. At the federal level, there is no uniform personal information protection legislation in the US, but the Federal Trade Commission (FTC) of the US ensures that consumers are entitled to know and consent to the use of their information data. Considering the risk of market failure, special legislation has been made for some specific sectors, such as the credit reporting sector and the health insurance sector.[19] This market economy and risk-based concept can explain why the US proposed, during the digital trade negotiations, that restricting the cross-border flow of personal information should be "necessary and proportionate to the risks presented." In fact, the US opposed the adoption of a "high standard" of personal information protection like that of the EU, but advocated that each country can protect it in its own way, and that "compatibility" should be promoted between different protection laws.

B. Safeguards against National Security Risks

In 2013, after the "Snowden Affair" disclosed "Prism" and other surveillance programs,[20] national security risks related to cross-border data flows have drawn increasing attention worldwide, and some countries have restricted or prohibited cross-border flows of data, which are related to personal information and non-personal information in sensitive fields such as finance and medical conditions. However, national security concerns have always been treated as "exceptions" in trade negotiations, and this point has been highlighted as the "national security exception" of WTO agreements.[21] However, given the fact that cross-border data flows have not been considered in the negotiation of WTO agreements,[22] and there is difficulty in citing the past WTO dispute settlements,[23] there is difficulty in citing the WTO security exceptions for supporting the restrictions of cross-border data for national security.

Most probably this is why recent digital trade agreements such as CPTPP and DEPA

---

[19] See Fair Credit Reporting Act of 1970 and Health Insurance Portability and Accountability Act of 1996.

[20] "Prism" is one of many surveillance programs by the US, which can collect data and information directly from the servers of the Internet companies. See Glenn Greenwald, 无处可藏 : 斯诺登、美国国安局与全球监控 (*No Place to Hide: Edward Snowden, the NSA and the USA Surveillance State*), translated by MI La and WANG Yong, China CITIC Press (Beijing), at 100–108 (2014).

[21] The General Agreement on Tariffs and Trade (GATT), the General Agreement on Trade in Services (GATS) and the Agreement on Trade-Related Intellectual Property Rights (TRIPS) all have clear provisions. See AN Baisheng, WTO 安全例外条款分析 (Analysis of WTO Security Exceptions), 3 国际贸易问题 (*Journal of International Trade*), 125–126 (2013).

[22] See PENG Yue, 数字贸易治理及其规制路径 (Digital Trade Governance and Its Regulation Path), 4 比较法研究 (*Journal of Comparative Law*), 160–161 (2021).

[23] See MA Guang, FTA 数据跨境流动规制的三种例外选择适用 (Application of Three Exceptions to the Regulation of Cross-Border Data Flow in FTA), 5 政法论坛 (*Tribune of Political Science and Law*), 17–19 (2021).

have introduced WTO security exceptions,[24] and provided special exceptions for cross-border data flows. Article 14.11 of CPTPP and Article 4.3 of DEPA both stipulate that, in principle, "each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person" (Paragraph 2), but the contracting party may adopt or maintain restrictions on the cross-border flow of information in order to achieve a legitimate public policy objective, as long as the measure "(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on transfers of information greater than are required to achieve the objective" (Paragraph 3).

In line with the WTO negotiating text, China and some other countries suggested introducing WTO general exceptions and security exceptions. The US suggested providing special exceptions for cross-border data flows consistent with CPTPP, but the US claimed that free data flow should be made more thorough compared with Article 14.11 of CPTPP, because the US no longer recognized that each Party in paragraph 1 of this Article "may have its own regulatory requirements," and the US revised that "each Party shall allow the cross-border transfer" into "No Party shall prohibit the cross-border transfer" in Paragraph 2 of this Article. With regard to the cross-border data flow in the EU, apart from the above-mentioned claim that all parties could take appropriate measures to protect personal information, the EU did not require WTO exception clauses or special exceptions. The EU primarily suggested prohibiting four kinds of data localization, including requiring the use of domestic computing facilities to process data, requiring local storage or processing of data in the domestic territory, prohibiting the storage or processing of data in other countries, and making the use of domestic computing facilities or data localization requirements a condition to allow data flow.[25]

Until now, the special exception of "legitimate public policy" has not been authoritatively explained, but it should be different from the national security exception of WTO and similar to the "public morality or public order" of the general exception of WTO in terms of expression and qualification conditions. Thus, it is necessary to "make clear the legal goal and necessity" and "ensure that the implementation of the

---

[24] Article 29. 2 of CPTPP and Article 15. 2 of DEPA stipulate that nothing in this Agreement shall be interpreted as: (a) requiring a contracting party to provide or allow access to any information that it determines would be contrary to its basic security interests if disclosed; or (b) prevent a contracting party from taking measures that it deems necessary to fulfill its obligation to maintain or restore international peace or security or to protect its own basic security interests.

[25] See WTO, *Electronic Commerce Negotiations—Consolidated Negotiating Text*, Annex 1 Scope and General Provisions, (6) general exceptions, (7) security exception; B. 2. Flow of information, Para. 6 Alt. 1, Para. 5 Alt. 1, and Alt. 3.

measures does not constitute discrimination or disguised trade restrictions," [26] yet meeting these requirements is quite difficult. Therefore, in the face of the increasingly severe national security challenge related to cross-border data flows, neither the WTO national security exception nor the "legitimate public policy" exception stipulated in the digital trade agreement can be used as legitimate bases for implementing universal regulation measures for cross-border data based on national security.[27]

It should be pointed out that the US advocates thorough cross-border data flow and the EU stands in resolute opposition to data localization. However, from the perspective of their domestic legislation, they both have various laws restricting cross-border data flows for the sake of their national security, and these laws are by no means just "exception clauses." In the US, for example, since 2010, the Controlled Unclassified Information Management System has been established.[28] Sensitive information in 20 categories and 125 subcategories, such as national defense, finance, intelligence and enforcement, other than classified information, are controlled according to their degrees of risk. One of the measures is "Not Releasable to Foreign Nationals" (NOFORN), taking the "National Defense" category of the information prohibited from sharing with foreign nationals as an example, including Unclassified Controlled Nuclear Information, National Disclosure Policy, etc. In August 2018, the Foreign Investment Risk Review Modernization Act was promulgated,[29] authorizing the Committee on Foreign Investment in the United States (CFIUS) to review foreign noncontrolling investments in US businesses involved in "sensitive personal data" in order to prevent these data from being acquired by foreign government or foreign entities. In May 2019, the US president Donald Trump issued the Executive Order "Securing the Information and Communications Technology and Services Supply Chain" [30] and implemented the "Clean Network" during his administration, prohibiting the trading and use of information technology and services of foreign adversaries that may threaten US national security, foreign policy and economy. In June 2021, Joe Biden' s administration issued the Executive Order "Protecting

---

[26] See SUN Nanxiang, 互联网规制适用 WTO 公共道德与秩序例外问题研究 (Research on the Application of Internet Regulation to the Exceptions of WTO Public Morality and Order), 6 国外社会科学前沿 (*International Studies of Social Sciences*), 25–29 (2019).

[27] Some scholars have pointed out that it will be difficult to justify measures to restrict data flows with exceptions. See SHI Jingxia, 数字经济背景下的 WTO 电子商务诸边谈判：最新发展及焦点问题 (On WTO E-Commerce under the Background of Digital Economy Judgment: The Latest Development and Focal Issues), 2 东方法学 (*Oriental Law*), 178 (2020).

[28] See "Executive Order 13556: Controlled Unclassified Information," 75 (216) *Federal Register*, 68675–68677 (November 9, 2010); Controlled Unclassified Information (CUI), 32 C. F. R. Part 2002.

[29] Foreign Investment Risk Review Modernization Act of 2018 (FiRRMA), Pub. L. No. 115–232,132 Stat. 2173.

[30] "Executive Order 13873: Securing the Information and Communications Technology and Services Supply Chain," 84 (96) *Federal Register*, 22689–22692 (May 17, 2019).

Americans' Sensitive Data from Foreign Adversaries," [31] which is designed to avoid sensitive data related to US national security from leaving the country.

C. Jurisdiction Requirements for Justice and Enforcement

The challenge of cross-border data flows to sovereign jurisdiction is a major concern that cannot be covered in the current digital trade negotiations. From the perspective of international law, specific embodiment of the state' s exercise of sovereignty is its jurisdiction over its territory and its nationals, primarily territorial jurisdiction and personal jurisdiction, supplemented by protective jurisdiction and universal jurisdiction and the state' s exercise of sovereignty can be divided into legislative, judicial, and enforcement jurisdiction.[32] The emergence and development of Internet technology have created cyberspace, in which large-scale cross-border data flows have significantly impacted traditional national sovereignty, especially enforcement jurisdiction, based on physical national boundaries and territorial jurisdiction. Thus, the idea of expanding national sovereignty began to appear, and concepts such as "information sovereignty" and "data sovereignty" [33] were suggested one after another. Countries have also introduced measures to safeguard sovereign jurisdiction, which to some extent constitute restrictions on the cross-border flow of data. These measures can be summarized into two categories:

The first is "blocking provisions," which prohibit overseas justice and enforcement agencies from obtaining data without consent of a host nation. For example, Articles 2702 and 2703 of the Stored Communications Act of the US, passed in 1986, stipulate that providers of electronic communication services (ECS) and remote computing services (RCS) to the public shall not intentionally disclose the communication content stored or carried in the services to any individual or entity, except under exceptional circumstances. For specific justice or enforcement purposes, only US government entities can request these two types of service providers to provide communication content or related records through search warrants, etc., under the statutory conditions.[34] The Act restricts the

---

[31] "Executive Order 14034: Protecting Americans' Sensitive Data from Foreign Adversaries," 86 (111) *Federal Register*, 31423–31426 (Jun. 11, 2021).

[32] See WANG Tieya, ed., 国际法 (*International Law*), Law Press (Beijing), at 76, 90 (1995). See James Crawford, *Brownlie's Principles of Public International Law*, 9th Edition, Oxford University Press (Oxford), at 440 (2019).

[33] See LIU Liantai, 信息技术与主权概念 (Information Technology and the Concept of Sovereignty), 2 中外法学 (*Peking University Law Journal*), 518–520 (2015); CAI Cuihong, 云时代数据主权概念及其运用前景 (Concept of Data Sovereignty in Cloud Age and Its Application Prospect), 12 现代国际关系 (*Contemporary International Relations*), 58–60 (2013); SHEN Guolin, 大数据时代的数据主权和国家数据战略 "Data Sovereignty and National Data Strategy in the Age of Big Data," 6 南京社会科学 (*Nanjing Journal of Social Sciences*), 114–116 (2014).

[34] See Title II Stored Wire and Electronic Communications and Transactional Records Access (Stored Communications Act), Electronic Communications Privacy Act of 1986 (ECPA), § § 2702–2703, Pub. L. No. 99–508, 100 Stat. 1860, 1861–1863.

enforcement of compulsory access to communication data to "US government entities," which actually prohibits US service providers from providing communication data stored in the US to foreign governments. Article 48 of the GDPR of the EU stipulates that any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to GDPR.[35]

The second is to ensure that the data of some important regulatory areas are stored in the domestic territory, and to ensure the justice and enforcement jurisdiction by "data localization." For example, in the process of promoting the formulation of CPTPP data cross-border flow clauses in the US, considering that the US treasury and financial regulatory agencies use localized storage of financial data as a regulatory option, they excluded financial data from the application scope of CPTPP.[36] As another example, in April 2018, India required all payment system providers to ensure that all data related to their system operations, including complete details of end-to-end transactions, were stored in systems within India, so that the Central Bank of India could "monitor and access the data stored by these system providers without restrictions, as well as the data stored by their service providers/intermediaries/third-party suppliers and other entities in the payment ecosystem." [37]

Faced with increasingly frequent cross-border data flows, some developed economies began to realize that blocking data access and data localization could not meet the practical needs. While advocating cross-border data flows, they began to expand their national jurisdiction and advocated "extraterritorial jurisdiction" over cross-border data.[38] Typical representatives are the EU and the US, but their approaches are different. Article 3 of the EU GDPR, based on the connection point of traditional personal jurisdiction and territorial jurisdiction, starts with the effect of data processing, and

---

[35] See General Data Protection Regulation, Art. 48. This article makes it clear that access to EU personal data for judicial enforcement can only be achieved through judicial assistance between countries.

[36] See Nigel Cory, "The TPP's Financial Data Carve Out—USTR Closes a Loophole for Digital Protectionists," Innovation Files Blog (Jul. 7, 2016), available at https://www.innovationfiles.org /the–tpps–financial–data–carve–out–ustr–closes–a–loophole–for–digital–protectionists (last visitied Jan. 25, 2022).

[37] See "RBI Notification on Storage of Payment Systems Data," RBI/2017–18 /153, Reserve Bank of India (April 6, 2018), available at https://www. rbi.org.in/scripts/NotificationUser.aspx?Id=11244 (last visited Jan. 25, 2022).

[38] In international law, extraterritorial jurisdiction is not a kind of independent jurisdiction. It can be understood that a country exercises sovereign power or authority outside its territory. See LIAO Shiping, 国内法域外适用及其应对——以美国法域外适用措施为例 (Extraterritorial Application of Domestic Law and Its Response—Taking Measures of Extraterritorial Application of American Law as an Example), 3 环球法律评论 (*Global Law Review*), 169 (2019).

includes both the processing of personal data outside the EU by institutions within the EU and the processing of personal data within the EU by institutions outside the EU. The Clarifying Lawful Overseas Use of Data Act[39] (hereinafter referred to as "CLOUD Act"), which was implemented in March 2018 in the US, no longer considers the territorial jurisdiction of data, but instead proposes a new model for governing the "data controller," stipulating that no matter whether the communication, record or other information is located in the US, ECS or RCS) providers in the US are obliged to keep, back up or disclose the communication contents and any records or other information of users or subscribers owned, supervised or controlled by them according to the statutory requirements. As a result, the data controlled by these service providers may be obtained by the US government, which significantly expands the jurisdiction of the US over overseas data.

Evidently, this kind of "extraterritorial jurisdiction" is a unilateral action. Although it is beneficial to alleviate the pressure of data localization, it inevitably conflicts with the existing "territorial jurisdiction" of data. Should this conflict of sovereign jurisdiction not be properly resolved, it would put multinational enterprises into the "vortex" of the conflict of jurisdiction,[40] and prompt the general requirements of relevant countries for "blocking access" and "data localization," which would further block the cross-border flows of data. To solve the national jurisdiction conflict related to cross-border data, it is urgent to explore multilateral cooperation on the basis of mutual respect for national sovereignty.

D. Face up the Common Legitimate Concerns

The above analysis has highlighted three non-economic concerns over regulations on cross-border data flows in major economies in the world, although these concerns differ in degree: protecting personal information, safeguarding national security, and ensuring sovereign jurisdiction. Nowadays, the digital trade negotiations initiated and designed by the US only cover some of these concerns. Except for the protection of personal information strongly advocated by the EU, concerns relating to national security are only regarded as "exceptions" of free trade, and justice and enforcement jurisdiction has received no attention at all. It appears that the digital trade negotiations are limited to digital trade. However, considering a large number of regulations and laws on data security and data jurisdiction enacted in the US, one can tell that the US has actively ignored the above concerns in the digital trade negotiations. The underlying reason behind this deliberate ignorance is that the US has leveraged "free flow of data" and "free

---

[39] Division V—CLOUD ACT, Consolidated Appropriations Act, 2018, Pub. L. No. 115–141, 132 Stat. 1213.

[40] See HONG Yanqing, "法律战"旋涡中的执法跨境调取数据：以美国、欧盟和中国为例 (Law Enforcement Cross-border Data Acquisition in the Vortex of "Legal War": Taking the United States, the European Union, and China as Examples), 1 环球法律评论 (*Global Law Review*), 41–42 (2021).

flow of trade" for steer the digital trade negotiations. By advocating thorough free cross-border flow of data, the US has supported its advanced digital technology enterprises in development of the global market, allowing massive data flows back to the US, thus maintaining its dominant position in the global digital market and cyberspace.

It should be pointed out that cross-border flow of data has triggered data protectionism at the economic level. With the development of the digital economy, data have become a national basic strategic resource, and countries have begun to compete for data resources. However, random competition has generated "data nationalism," so India emphasized the necessity of promoting data localization and developing the digital industry from the perspective of data nationalism.[41]From the perspective of national economic development and national strategy, a certain degree of data defensiveness is acceptable.[42] However, it is a kind of digital trade protectionism to willfully restrict cross-border flow of data only from the national interests, and this should be resolutely opposed. This paper holds that both economic and non-economic concerns may require data localization, and judgement of its legitimacy should start with the purpose and degree of regulation, which cannot be simplistically generalized.

In short, the current digital trade negotiations cannot cover all the issues related to cross-border data flows, and cannot reach the critical consensus globally. To explore the global regulatory framework, it is urgent to study the above legitimate concerns and deliberate them thoroughly.

II. China's Exploration of Promotion and Control of Cross-Border Data Flows

China has long recognized the limitations of discussing cross-border data flow only from the trade perspective. In 2019, the original proposal of WTO e-commerce plurilateral negotiations also emphasized that e-commerce should be defined as cross-border trade in goods enabled by the internet, together with relevant payment and logistics services; the issues such as cross-border data flow are complex and sensitive, and more exploratory discussions are needed.[43] Based on such broader profound understanding, China has recently put forward a new concept and paradigm of "secure cross-border data flow," has launched the Global Initiative on Data Security, and has explored the construction of control system for overseas transfer of data. Before 2017, China applied administrative regulations, departmental rules, and normative documents for overseas transfer of data in specific fields, such as finance, credit, population health, internet maps, and online taxi

---

[41] See MAO Weizhun & LIU Yishen, 数据民族主义：驱动逻辑与政策影响 (Data Nationalism: Driving Logic and Policy Impact), 3 国际展望 (*Global Review*), 23–25 (2020).

[42] See LIU Jinhe & CUI Baoguo, 数据本地化和数据防御主义的合理性与趋势 (Rationality and Trend of Data Localization and Data Defense), 6 国际展望 (*Global Review*), 99 (2020).

[43] See WTO, *Joint Statement on Electronic Commerce—Communication from China*, INF /ECON/19, Apr. 24, 2019.

booking.[44] After 2017, China promulgated the Cybersecurity Law, Data Security Law, and Personal Information Protection Law, and established a comprehensive control system for overseas transfer of data.

A. The Concept of Secure Cross-Border Data Flow

Based on the Cybersecurity Law, "the orderly and free flow of network information according to law." The Data Security Law establishes the value concept and basic principle of "secure cross-border data flow," which can be understood from two aspects: paying equal attention to data protection and utilization; and coordinating the rule of law at home and abroad.

1. Paying Equal Attention to Effective Protection and Legal Utilization. Article 11 of the Data Security Law clearly stipulates that the state shall "promote the secure and free cross-border flow of data." The "free" here should be understood together with Article 7, "the orderly and free flow of data according to law." Hereby, "orderly according to law" is the core, and "free" is just a continuation from the similar expression of "Cybersecurity Law," which is used to describe the "flowing" state of data and to highlight the legislative value of "promoting data development and utilization." Actually, it does not have much regulatory significance. Therefore, for cross-border data flow, China's core regulatory concept is to ensure the "secure flow" of data.

Article 3 of the Data Security Law defines data security as "taking necessary safeguards to ensure that data are in a state of effective protection and legal utilization, and have the ability to guarantee a continuous security state." From the expression point of view, emphasis is placed on ensuring equal attention to data "effective protection" and "legal utilization." The author believes that "effective protection" and "legal utilization" correspond to "data self-security" and "data utilization security" respectively. Data self-security is the integrity, confidentiality and availability of data itself and these emphasize the traditional concept of data security. Data utilization security emphasizes risk prevention using large-scale aggregation and analysis of data.[45] In fact, data security conforms to the actual demand of large-scale data flow and utilization in the era of the digital economy, and significantly expands the connotation of "data security."

Based on this new concept, the Data Security Law has established a new paradigm of

---

[44] Some relevant regulations include Notice of the People's Bank of China on Banking Financial Institutions Doing a Good Job in Protecting Personal Financial Information (2011), Regulations on the Administration of Credit Information Industry (2013), Measures for the Administration of Population Health Information (for Trial Implementation) (2014), Regulations on Map Management (2016), and Interim Measures for the Administration of Online Taxi Booking Business Operations and Services (2016).

[45] See LIU Jinrui, 数据安全范式革新及其立法展开 (The New Data Security Paradigm and Data Security Legislation), 1 (*Global Law Review*), 10 (2021).

paying equal attention to data self-security and data utilization security. While promoting data development and utilization, the Data Security Law has made a principled regulation relating to data utilization security, emphasizing that conducting data processing activities "shall be conducive to promoting economic and social development, enhancing people' s well-being and conforming to social morality and ethics," and "shall neither endanger national security and public interests, nor harm the legal rights and interests of individuals and organizations." To ensure the secure cross-border flow of data means to ensure the self-security of the flowing data, and also to ensure that the cross-border data meets the requirements of this kind of utilization security. The Global Initiative on Data Security clearly states that countries should not use the data to conduct activities that undermine other States' national security and public interests.

2. Coordinate Domestic Rule of Law and Foreign-Related Rule of Law. Cross-border data flow is a global issue related to national data security. To participate in the formulation of relevant international rules, a holistic approach to national security must be adhered to, and domestic rule of law and foreign-related rule of law must be coordinated. China has launched the Global Initiative on Data Security, which is a specific measure to pursue a holistic approach to national security, "build a community with a shared future, and push all parties to move towards the goal of mutual benefit and common security," [46] and promote the formation of international consensus. It includes the proposition of secure cross-border data flow as follows.

(1) On safeguarding national security. States should handle data security in a comprehensive, objective and evidence-based manner, and stand against ICT activities that impair other States' critical infrastructure or steal important data, or use the data to conduct activities that undermine other States' national security and public interests.

(2) For protection of personal information. States should take actions to prevent and put an end to activities that jeopardize personal information through the use of ICTs, and oppose mass surveillance against other States and unauthorized collection of personal information of other States with ICTs as a tool.

(3) In regard to data localization. States should encourage companies to abide by laws and regulations of the State where they operate. States should not request domestic companies to store data generated and obtained overseas in their own territory.

(4) On cross-border data request for justice and enforcement. States should respect the sovereignty, jurisdiction and governance of data of other States, and shall not obtain data located in other States through companies or individuals without other States' permission. Should States need to obtain overseas data out of law enforcement requirement such as combating crimes, they should do it through

[46] 坚持总体国家安全观，走中国特色国家安全道路 (Adhere to a Holistic Approach to National Security and Take the Road of National Security with China Characteristics), 人民日报 (*People's Daily*) , Apr. 16, 2014.

judicial assistance or other relevant multilateral and bilateral agreements. Any bilateral data access agreement between two States should not infringe upon the judicial sovereignty and data security of a third State.

B. The Dual-Track Multi-Layer Regulatory System

According to the provisions of Cybersecurity Law, Data Security Law, and Personal Information Protection Law, China has set up two independent systems for overseas transfer of data based on different concerns of cross-border data flow, with "important data" and "personal information" as the starting points. Firstly, the control system for overseas transfer of important data to safeguard national security is primarily stipulated in Data Security Law and Cybersecurity Law. The second is the system of cross-border provision of personal information for the protection of personal rights, which is primarily stipulated in the Personal Information Protection Law. There are significant differences between the two systems in regulatory objectives, applicable scope, and regulatory means, forming a "parallel dual-track" model. In these two systems, different subjects are distinguished, such as critical information infrastructure operators, important-data processors, and processors who process the personal information up to a specified amount, and different scene-based rules, such as cross-border data request for justice and enforcement, are stipulated, showing the characteristics of "multi-layer regulation." The main points are summarized as follows:

1. Control System for Overseas Transfer of Important Data to Safeguard National Security. To safeguard cyberspace sovereignty and national security, the Cybersecurity Law draws lessons from overseas experience and establishes a protection system for critical information infrastructure. Article 37 specializes in the control of overseas transfer of important data of critical information infrastructure and emphasizes that: personal information and important data collected and produced by critical information infrastructure operators during their operations within the territory of China shall be stored within China; if it is indeed necessary to provide such information and data to overseas parties due to business requirements, security assessment shall be conducted in accordance with the measures developed by the national cyberspace administration in conjunction with relevant departments of the State Council, unless it is otherwise prescribed by any law or administrative regulation.

Considering that the overseas transfer of important data is not only limited to critical information infrastructure, the Data Security Law has expanded the application scope of control system for overseas transfer of important data to all important-data processors according to the needs of practical development and data security management. Article 31 clearly stipulates: the security management of cross-border transfer of important data collected and generated by operators of critical information infrastructure during their operations in the territory of China shall be governed by the Cybersecurity Law; and

the measures for the security management of cross-border transfer of important data collected and generated by other data processors during their operations in the territory of China shall be developed by the national cyberspace administration in conjunction with the relevant departments of the State Council. In addition, in conjunction with the Export Control Law, Article 25 stipulates the data export control system: "The state shall impose export control in accordance with the law on data as controlled items related to safeguarding national security and interest and performing international obligations."

For the control system for overseas transfer of important data, the Cybersecurity Law and Data Security Law only provide the basic framework, while the specific system design needs to be defined by supporting regulations. Article 73 of the Regulation on the Administration of Network Data Security (Draft for Collection of Comments) (hereinafter referred to as "Draft Regulation for Comments") issued by the Cyberspace Administration of China in November 2021 defines the key "important-data" connotation and extension, stipulating that "important data refer to data that may endanger national security and public interest if it is tampered with, destroyed, leaked or illegally obtained or used," and providing a list of seven important data. However, this Draft Regulation for Comments is too general to be workable. In October 2021, the Cyberspace Administration of China issued the "Measures of Security Assessment of the Overseas Transfer of Data (Draft for Comments)," which detailed rules for security assessment of overseas transfer of important data. The assessment items include: legality, justification and necessity of the aim, scope and method of overseas transfer of data; quantity, scope, category and sensitivity of the data to be transferred abroad; risks to national security and public interests may caused by the overseas transfer of data; risks to data leakage, damage, tampering and abuse caused by the overseas transfer and subsequent transfer of data.

2. System of Cross-Border Provision of Personal Information for Protection of Personal Rights and Interests. To protect the rights and interests relating to personal information and to meet the practical needs of the increasingly frequent cross-border flow of personal information, Chapter 3 of the Personal Information Protection Law stipulates the system of cross-border provision relating to personal information, which primarily includes:

First, the legal means concerning cross-border provision regarding personal information have been defined. These legal means include security assessment organized by the national cyberspace administration in specific situations, personal information protection certification by professional institutions, conclusion of a standard contract with the overseas recipient, meeting other conditions stipulated by laws or administrative regulations or by the national cyberspace administration, and in accordance with international treaties concluded or acceded to by China.

Second, personal information processors are required to take necessary measures to ensure that the overseas recipient' s personal information processing activities meet the personal information protection standards stipulated in this Law.

Third, the "notification and consent" for cross-border provision of personal information should be more strictly regulated, and individuals' separate consent should be obtained.

Article 40 of the Protection of Personal Information Law stipulates: critical information infrastructure operators and the personal information processors that process the personal information reaching the threshold specified by the national cyberspace administration in terms of quantity shall store domestically the personal information collected and generated within the territory of China; where it is truly necessary to provide the information to an overseas recipient, the security assessment organized by the national cyberspace administration shall be passed; where laws, administrative regulations, or provisions issued by the national cyberspace administration provide that security assessment is not required, such provisions shall prevail. The reason for this Article is that the personal information involved in the critical information infrastructure and a huge amount of personal information collection may affect national security, so its overseas transfer should pass the security assessment organized by the national cyberspace administration as is the case for overseas transfer of important data.

In addition to the provisions of Article 40 "Security Assessment" in the aforementioned "Measures of Security Assessment of the Overseas Transfer of Data (Draft for Comments)," the detailed rules for cross-border legal channels for personal information such as certification by professional institutions and conclusion of standard contracts are yet to be established.

3. System of Cross-Border Data Request for Justice and Enforcement under the Sovereign Jurisdiction. With regard to cross-border data request for justice and enforcement, China has always advocated that the principle of respecting the sovereign jurisdiction of all countries should be followed, and the Global Initiative on Data Security reiterates this principle. Article 36 of the Data Security Law and Article 41 of the Personal Information Protection Law both implement this principle and continue the cross-border legal assistance model of the International Criminal Legal Assistance Law adopted in 2018, and their expressions are basically the same. Specifically, the competent authority of China shall process a request for data/personal information stored within China's territory from a foreign judicial or law enforcement authority in accordance with relevant laws and international treaties and agreements entered into or acceded to by China, or under the principle of equality and reciprocity; without the approval of the competent authority of China, a domestic organization or individual shall not provide data/personal information

stored within China's territory to any foreign judicial or law enforcement authority. Article 48 of the Data Security Law also specifies severe penalties for non-compliance with such requirements, so as to "provide relevant organizations and individuals with a sufficient legal basis to refuse unreasonable foreign requests for locally available data and personal information." [47]

In addition, after the Snowden Affair came to light, the abuse of public power to obtain data held by private entities has become the focus of attention of all countries. To dispel concerns of other countries about cross-border data request for justice and enforcement by China, Article 35 of the Data Security Law regulates the behavior of China's justice and enforcement agencies in the request of data: a public security authority or national security authority shall legally request data in accordance with relevant provisions issued by the state and by strictly following approval procedures as needed for maintaining national security or investigating crimes.

C. China's Continuing Exploration of Cross-Border Data Flow Management

To sum up, as far as cross-border data flow is concerned, China adheres to the concept of "secure flow" and builds a hierarchical institutional framework of "parallel dual-track" for the regulation of overseas transfer of "important data" and "personal information." China's rules of cross-border provision of personal information, drawing on the experience of extraterritorial legislations, provide a variety of legal means for cross-border personal information flow while strengthening the protection of personal rights and interests, and this is conducive to promoting China's integration with other economies and developing China's digital economy. The exploration of China's control system for overseas transfer of important data has significantly advanced the legal framework of regulating cross-border data flows based on national security concerns, and this provides a new institutional option for the global response to the national security challenges related to cross-border data flows.

However, it needs to be pointed out that at present, China has only legally stipulated the institutional framework of "dual-track" control, and the supporting system is far from perfect. The core rules such as scope of important data and security assessment of the overseas transfer of data are still unclear, which not only affects China's data flow and trade flow, but also easily leads to misunderstanding and accusations that China hinders data flow and creates trade barriers on the grounds of "security." From the perspective of globalization, China's current system design mostly focuses on "data outflow"

---

[47] 全国人民代表大会宪法和法律委员会关于《中华人民共和国数据安全法 (草案)》修改情况的汇报 (Report of the Constitution and Law Committee of the National People's Congress on the Amendment of People's Republic of China (PRC) Data Security Law [Draft Case]), China National Net, available at http://www.npc.gov.cn/npc/c30834/202106/6afa1aa6b29e431db28b5a659ed27b83.shtml (last visited Jan. 25, 2022).

for avoiding improper data acquisition, and the regulatory measures are mostly pre-supervision and basically defensive, without considering the impact of these regulatory measures on "data inflow" synchronously. In the long run, this system design cannot meet the practical needs of China's digital economy development, and cannot adapt to China's overall approach in the current round of globalization of the digital economy. In brief, China's cross-border data flow system still has much room for improvement.

III. China's Approach Regarding Exploration of a Global Regulatory Framework for Cross-Border Data Flows

Given the global challenges in cross-border data flows, the current digital trade negotiations that only focus on the economic dimension cannot accommodate all regulatory concerns. There are big differences among countries on non-economic concerns such as protecting personal information, safeguarding national security, and ensuring sovereign jurisdiction. The global regulations on cross-border data flow have shown signs of "fragmentation," and there is an urgent need to explore and formulate a new regulatory framework. In this regard, China has been actively participating in regional or bilateral negotiations, and has formally applied to join CPTPP and DEPA, making efforts to "catch up" and "advance side by side," and this deserves high recognition.

Furthermore, it is necessary for China to start with the non-economic common concerns of cross-border data flows, to put forward a new topical framework and systematic proposition beyond the trade negotiations in combination with its own exploration, to promote the generation of new international rules based on the gained multilateral consensus, and to strive to "lead" in exploring international rules of digital governance. Therefore, this paper lays out the following suggestions on the basic philosophy and compatibility framework for global regulation of cross-border data flows.

A. The Basic Philosophy of Global Regulatory Framework for Cross-Border Data Flows

Non-economic concerns arising from cross-border data flows are epitomized most in cyberspace sovereignty conflicts. Only by respecting each other's sovereignty, can consensus and cooperation be fully made through multilateral consultation, and can Lawrence Lessig' s "Competing Sovereignty" in cyberspace be transformed into "Interdependent Sovereignty." [48] As such, China's proposal of "Respecting Cyber Sovereignty, Building a Community with a Shared Future in Cyberspace" should be the basic premise for the exploration of the global regulatory framework for cross-border data flows. On this premise, this paper summarizes the regulatory consensus and legislative experience of major countries and outlines the basic philosophy for a proposed global

[48] See Lawrence Lessig, 代码 2.0：网络空间中的法律 (*Code 2.0: Law in Cyberspace*), translated by LI Xu & SHEN Weiwei, Tsinghua University Press (Beijing), at 299–333 (2009).

regulatory framework.

1. Promotion of Legitimate and Controllable Cross-Border Data Flow. From the perspective of data flow promoting trade flow, it seems that free data flow should be promoted unconditionally. But just as free trade applies regulation to exceptional cases, data flow also needs regulation, not to mention that cross-border data flows not just promote trade and economy. Based on non-economic concerns such as national security, personal rights protection, and sovereign jurisdiction, countries have adopted different regulatory measures for cross-border data flows, and there is no unrestricted free flow of data in the world. As opposed to the free cross-border flow of data, China has put forward the concept of "secure cross-border flow" of data cross border, which considers these regulatory concerns.

What needs to be pointed out is that the "security" of "secure cross-border data flow" has actually gone beyond the traditional understanding of data security. As mentioned above, it also includes data utilization security in its connotation. This kind of security emphasizes the legitimacy and controllability of large-scale data flow and utilization in the digital economy era.[49] The legitimacy and controllability can completely cover regulatory concerns such as personal rights protection and national sovereign jurisdiction. However, from the semantic point of view, the foreign understanding of "data security" still remains in the traditional paradigm regarding data integrity, confidentiality, and availability, which easily leads to a foreign misunderstanding that China creates obstacles and barriers on the grounds of "security." Therefore, in order to accurately express regulatory concerns and make it more widely acceptable, it is suggested that "secure flow" should be upgraded to "legitimate and controllable flow," and "promoting legitimate and controllable cross-border data flow" should be taken as the basic concept of a global regulatory framework.

In addition, "legitimate and controllable cross-border data flow" emphasizes objectivity and inclusiveness more than "data free flow with trust" as put forward in the 2019 G20 Osaka Digital Economy Declaration. "Trust" often refers to the closeness of the relationship between the two sides, and it is easy to slide into the dichotomy of "friend" and "opponent," which becomes an excuse for engaging in exclusive "small circle" and unilateralism and protectionism. "Legitimate and controllable" starts with the legitimacy of regulation, which is more conducive to the global regulatory framework for win-win cooperation.

2. Categorized Supervision Based on Risk Concerns. Legitimate and controllable cross-border data flow emphasizes the controllability of risks, which requires a risk-based regulation method. Generally, risk control includes four strategies: accepting

[49] See LIU, fn. 45 at 11.

risk, avoiding risk, controlling risk, and transferring risk.[50] Avoiding risks, controlling risks and transferring risks often correspond to pre-supervision, in-process supervision and post-supervision. These three strategies and supervision cannot achieve absolute security, so regulating risk should mean accepting certain risks, which is also the reason for coordinating the relationship between security and development. From this point of view, both the US "Clean Network" and the Indian extreme data nationalism are irrational decisions trying to block the cross-border flow of data for seeking so-called absolute security for themselves. Moving towards a global regulatory framework for cross-border data flows actually involves achieving relative common security through multilateral cooperation.

Risk-based regulation needs to match different supervision methods according to the degree of risk and conduct categorized supervision. As for the category of supervision, this paper believes that in addition to considering the degree of risk in combination with data categorization and hierarchy, we should also consider the different concerns of regulating the cross-border flow of data. China's "dual-track" model, which distinguishes the control of overseas transfer of important data from the cross-border provision of personal information, actually takes into account the different concerns of safeguarding both national security and personal rights and interests. Considering that these two concerns have been generally recognized at present, this "dual-track" distinction can be used as the basis for the discussion of the global regulatory compatibility framework. OECD has summarized the control methods of cross-border data flows into four basic categories: no regulation, ex-post accountability, flows conditional on safeguards, flow conditional on ad-hoc authorization.[51] A "gradient regulatory spectrum" of weak-to-strong control has been formed.[52] For the cross-border flows of various categories of data, the appropriate method should be chosen to use within this regulatory spectrum, with the establishment of a regulatory system based on pre-supervision, in-process supervision and post-supervision. It is necessary to prevent the indiscriminate "one size fits all" practice of pre-supervision to avoid undue obstacles to data flows.

3. Coordinate the Rule of Law at Home and Abroad to Promote System Compatibility. Cross-border data flows mean both "transfers of data outside the territory" and "transfers of data into the territory," requiring two kinds of jurisdictions: domestic rule of law and foreign rule of law. Any country participating in the globalization of the digital economy

---

[50] See US Department of Homeland Security, "Risk Management Fundamentals," 23 (Apr. 2011), available at https://www.dhs.gov/sites/default/files/publications/rma–risk–management–fundamentals.pdf (last visited Jan. 25, 2022).

[51] See OECD, "Trade and Cross–Border Data Flows," 16–21 (Jan. 2019), available at https://doi.org/10.1787/b2023a47–en (last visited Jan. 25, 2022).

[52] See XU Ke, 自由与安全：数据跨境流动的中国方案 (Freedom and Security: China's Scheme for Cross-Border Data Flow), 1 环球法律评论 (*Global Law Review*), 26 (2021).

needs to look at transfers of data both outside the territory and into the territory as well as two kinds of jurisdictions as a whole. Given the common challenges of cross-border data flows, countries have common concerns about national security, personal rights protection, sovereign jurisdiction, etc., although they have different understandings on some issues due to their differences in basic national conditions, development stages, and cultural traditions. Exploring the rule of law in response to these common concerns is worthwhile for countries to learn from each other, based on the varying national conditions. The mechanism for cross-border flow of personal information stipulated by the EU (GDPR), such as binding corporate rules and standard contracts, has been widely recognized by other countries, but the recognition of "adequacy decision" is limited. The reason is that although the EU has been firmly opposed to data localization in digital trade negotiations; its "high standard" protection together with strict "adequacy decision" which has been obtained by few countries or regions, has resulted in de facto localization requirements, and is not conducive to the cross-border data flows.

Even with the same concerns, there is no universal regulatory system. When different countries have different system designs on the same issue, we should try our best to achieve system compatibility. From the normative level where there is consensus, promoting system compatibility can be divided into three scenarios: Firstly, there is consensus at the specific system level, and common rules, such as bilateral agreement of data request for justice and enforcement, can be reached through consultation. Secondly, there is consensus only at the level of basic principles, and the minimum regulatory standards that all parties would abide by can be established through consultation. For example, CPTPP recognizes that all parties can maintain existing measures to protect users' personal information. Thirdly, there is consensus only at the level of values. In this case, it should be realistically acknowledged that compatibility cannot be achieved at the institutional level, but consultation and dialogue can be maintained on common concerns, such as the discussion of data related to national security. Therefore, it is particularly important to design a compatible framework for the global regulation on cross-border data flows. This kind of framework should start from common concerns, reflect the consensus of values and concepts, incorporate the consensus of basic principles, and guide the discussion in reaching institutional consensus.

B. Exploration of Compatible Framework of Global Regulatory Framework for Cross-Border Data Flows

To explore the compatible global regulatory framework for cross-border data flows is to find the "common law" of cross-border data flows. The so-called common law, from the perspective of comparative law, is a common solution or common principle or relatively ideal framework that can be applied to the same legal issues arising from

various legal orders.[53] As the digital economy globalization has experienced difficulty in going through "counter-current" and "perilous shoal" events, and while the digital trade negotiations led by Western countries cannot cover common concerns such as national security and sovereign jurisdiction, it is essential to explore this common law in order to avoid the "fragmentation" of global digital governance.

According to this common law discussion based on the above-mentioned basic philosophy, combined with the current regulatory consensus and institutional exploration, this paper holds that the global regulatory compatibility framework of cross-border data flows should cover three aspects: preventing national security risks, protecting personal information rights and interests, and safeguarding justice and enforcement jurisdiction. The following suggestions are put forward on how to promote the compatibility of different national rules and achieve the "common law" in these three aspects. Although these suggestions focus on improving China's cross-border data control system, the construction of this system from a global perspective can also be considered as a "China's Approach" based on China's domestic law to move towards a global regulatory framework for cross-border data flows.

1. Prevention of National Security Risks: Clarification of the Scope of Important Data to Define the "Negative List". As mentioned above, the digital trade negotiations currently pioneered by Western countries, whether introducing WTO national security exceptions or providing special "legitimate public policy" exceptions, are not sufficient as a legitimate basis for implementing universal regulatory measures for cross-border data based on national security. China has established the control system for overseas transfer of important data, and has significantly developed the legal framework based on national security for regulation of cross-border data flows. However, because the scope of important data has not been clarified yet, it has not only sparked unnecessary misunderstanding but has also affected China's data flow and trade flow. This has hindered China in presenting national security concerns based on important data internationally. Thus, it is suggested improving the control system for overseas transfer of important data at both international and domestic levels.

At the international level, controlling important data for safeguarding national security and public interest should be listed as a separate topic, no longer as part of an "exception clause." In the negotiation of digital trade, the EU practice of juxtaposing personal data and privacy protection clause with cross-border data flow clause can be used as a basis for drafting and initiating a separate "important-data clause." Those measures which restrict data flow and meet requirements of this "important-data clause," should not be treated as exceptions to free trade any more, leaving enough regulatory space for China and other countries with similar concerns. Considering the integrity of the system, we can propose

---

[53] See Ooki Masao, 比较法 (*Comparative Law*), translated by FAN Yu, Law Press (Beijing), at 72 (1999).

that the "national core data" stipulated in the Data Security Law is applicable to the national security clause of WTO, thus being distinguished from the "important-data clause." In view of the fact that important data may seriously affect national security and public interests, we should prioritize pre-supervision and rely on the current security assessment system of the overseas transfer of data. As far as system compatibility is concerned, it is difficult to reach a consensus, because important data concern national security, and countries should be free to determine their own specific scope of important data.

At the domestic level, under the guidance of the holistic approach to national security, the scope of important data should be clarified as soon as possible, and the security assessment system of overseas transfer of important data should be introduced as soon as possible, so as to define the "Negative List" of cross-border data flow of China. The definition of important data in Article 73 of "Draft Regulation for Comments" adopts the form of "generalization + enumeration," but the judgment standard of "possibly endangering national security and public interests" is too general. The seven categories of data listed in the "Draft Regulation for Comments" are logically overlapping, unclear in connotations, and mostly negligent in degrees of data importance. It is suggested to further clarify the connotation of "important" from the degree of harm, and reword the judgment standard of important data as that "may seriously harm the national security and public interest." Given the complexity of different industries and fields, it is impossible to specify the scope of important data in legislation, but possible to specify the identification system of important data. According to Article 21 of the Data Security Law, the national data security coordination mechanism should firstly coordinate the relevant departments to formulate a catalog of important data at the national level, and then each region or department should determine the specific catalogs of important data in the region or department and in the relevant sectors and fields. The responsible department, standard basis, and corresponding procedures for the identification of specific catalogues of important data in each sector or field should be specified. When the competent department develops the specific catalogue of important data, they can mainly require data processors to make a self-declaration according to the relevant standards, then they audit and confirm it. In addition, they can take the initiative to identify important data, and define legal liability for any subject who should declare but fail to declare their important data.

2. Protecting Personal Information Rights and Interests: Improvement of the Cross-Border Accountability to Ease the Pre-Supervision Pressure. Up to now, most countries have developed some degree of personal information protection system. For cross-border personal information protection, the core issue is how to promote the compatibility of different protection systems when personal information flows in countries or regions with different levels of protection. Now there are two protection practices: Firstly, the pre-supervision mechanism, whose typical case is the EU' s "adequacy decision" and "appropriate safeguards" ; secondly, the ex-post accountability mechanism,

whose typical case is the Cross-border Privacy Rules (hereinafter referred to as "CBPR") System of Asia-Pacific Economic Cooperation (APEC) advanced by the US.[54]

In 2011, APEC adopted the CBPR based on its privacy framework. The CBPR is a voluntary certification system, and enterprises that join the system for cross-border data flow must implement a set of privacy policies in line with APEC' s privacy framework to meet the requirements of accountability, notification, selection, security protection, and consumer rights. The system requires that the country where the enterprise is located has at least one Accountability Agent recognized by APEC, which certifies the compliance of the enterprise according to APEC privacy protection standards and is responsible for investigating consumer complaints. At least one Privacy Enforcement Authority has joined the APEC Cross Border Privacy Enforcement Arrangement (CPEA), which serves as the backing for dispute resolution and promotes the interoperability of privacy enforcement authorities in various economies.[55]

Comparing GDPR with CBPR, one can note a big difference between them in the level of compatible protection. GDPR is actually "favoring higher protection level rather than a lower one" when both are available, and if adequate protection is not achieved, the countries or regions concerned have to "stay abreast" with the EU protection level through adopting appropriate safeguards. On the other hand, CBPR is "favoring a lower protection level rather than higher one" when both are available, and it can be "accepted" by simply recognizing the APEC CBPR framework, which is actually the minimum standard for all parties to abide by. The two frameworks have their respective advantages and disadvantages: The GDPR-compatible mechanism costs more, but once it has been granted the adequacy decision, the cross-border flow of data is more convenient for enterprise. The threshold of CBPR compatibility is low and easy for enterprises to reach, but it is primarily based on voluntary certification with limited regulatory strength.

Personal Information Protection Law of China refers to the pre-supervision mechanism of GDPR, which stipulates the methods of certification by professional institutions and the conclusion of standard contracts. However, it does not adopt the mechanism of "adequacy decision," and only requires the personal information processor to take necessary measures to ensure that the protection level of the overseas recipient meets the protection standards of this Law. It seems that China has adopted the approach of accountability. Regarding the compatibility of China's rules of cross-border provision of personal information with those of other countries, it has been suggested that China can

---

[54] See XU Duoqi, 个人数据跨境流动规制的国际格局及中国应对 (International Pattern of Personal Data Cross-border Flow Regulation and China's Response), 3 法学论坛 (*Legal Forum*), 134 (2018).

[55] See APEC, *APEC Cross—Border Privacy Rules System: Policies, Rules and Guidelines*, updated as of November 2019, available at http://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019.pdf (last visited Jan. 25, 2022).

learn from the practices of the EU and the US, adopt both the pre-supervision mechanism and the ex-post accountability mechanism, and consider establishing a "White List" system in bilateral or multilateral negotiations according to the principle of reciprocity. Considering the pressure of pre-supervision, and the need for in-process supervision and post-supervision, and the cost of certification by professional institutions in the pre-supervision mechanism, we should also study and improve the accountability mechanism of overseas processors synchronously, so as to avoid undue obstacles to data flow due to excessive reliance on the pre-supervision mechanism. This ex-post accountability mechanism should be included in bilateral or multilateral mutual legal assistance treaties concluded between China and other countries, so as to avoid insufficient regulation of a voluntary certification system like CBPR. In addition, for the sake of scientific research such as vaccine research, we should also consider formulating special rules for the overseas transfer of personal information in scientific research fields.

3. Upholding Justice and Enforcement Jurisdiction: Focusing on Data Access Rights Instead of Relying on Data Localization. Judging from the jurisdiction of a country's justice and enforcement, one can note two aspects of data request: domestic data request by other countries and overseas data request by this country. In both aspects, there will be a conflict between the countries in sovereign jurisdiction. Moreover, with the development of big data, cloud computing, and other applicable technologies in recent years, cross-border data flow has become the norm, and jurisdictional conflicts have become increasingly frequent, resulting in a large number of phenomena such as "blocking access" and "extraterritorial jurisdiction." Some countries are concerned that they cannot exercise jurisdiction when data flows out of their own countries and thus have required "data localization." The system compatibility between jurisdictions is primarily the conclusion of bilateral or multilateral mutual legal assistance treaties (MLAT) on the premise of mutual respect for sovereignty. However, the traditional legal assistance procedure needs to be communicated and handled by the specialized agencies of both sides, which is often complicated, lengthy, and inefficient, and has become increasingly unsuitable for the development of digital economy globalization and the rapid resolution of disputes.

In this case, the mode of directly requesting data from the "data controller" defined in the CLOUD Act has emerged, which has significantly improved the efficiency of justice and enforcement. After the CLOUD Act was introduced, the EU Proposal for a Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters in April 2018[56] and the UK Crime (Overseas Production Order) Act in February

[56] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters,17. 4. 2018, COM (2018) 225 final.

2019[57] all adopted a similar model. The CLOUD Act has had various unreasonable restrictions on foreign governments' access to the data of "data controller" in the US, and it has been widely criticized.[58] However, its legislative attention to data access for meeting the requirements of the times deserves recognition. It is worth noting that in the US-Mexico-Canada Agreement (USMCA) reached in 2019, the US also abandoned its previous insistence on localized storage of financial data, and instead emphasized ensuring the access of regulators to relevant data. Article 17.18 of Chapter 17, "Financial Services" of the Agreement, provides that the Parties recognize that immediate, direct, complete, and ongoing access by a Party's financial regulatory authorities to information of covered persons, including information underlying the transactions and operations of such persons, is critical to financial regulation and supervision, and recognize the need to eliminate any potential limitations on that access.

In fact, should two countries enter into a bilateral mutual legal assistance treaty on the basis of fully respecting sovereignty and recognizing each other' s extraterritorial jurisdiction, even if the data concerned have not been stored in their own territory, as long as the data' s immediate, direct and complete access is guaranteed, then it will not compromise justice and enforcement. In other words, for cross-border data request by justice and enforcement, the location of data storage is not the key. Instead, the right to data access is the key. Certainly, to guarantee this kind of data access, legal liability for the obligor should be specified in case that he or she fails to make data access available per request in time. Thus, data localization required by justice and enforcement jurisdiction can be significantly reduced. It is suggested that China should explore establishing such data access mechanisms in bilateral or multilateral mutual legal assistance treaties with other countries.

Acknowledgements This article is funded by National Social Science Foundation's general project "Theoretical and Practical Research on International Criminal Judicial Assistance in Combating Cybercrime" (Project No.: 19BFX073); National Social Science Foundation's major project "Translation, Research and Database Construction of Cyberspace Policies and Regulations" (Project No.: 20 & ZD179).

[57] Crime (Overseas Production Orders) Act 2019.

[58] See KONG Qingjiang & YU Huayi, 数据立法域外适用现象及中国因应策略 (Extraterritorial Application of Data Legislation and China's Countermeasures), 8 法学杂志 (*Law Science Magazine*), 84 (2020).