Data Sovereignty Construction in International Trade Agreements: Causes, Models, and China's Choices

— *Based on the Study of Cross-border Data Flow Rules*

ZHANG Qianwen[*]

Abstract: *The Fourth Industrial Revolution has endowed the concept of state sovereignty with new era-specific connotations, leading to the emergence of the theory of data sovereignty. While countries refine their domestic legislation to establish their data sovereignty, they are also actively engaging in the negotiation of cross-border data flow rules within international trade agreements to construct data sovereignty. During these negotiations, countries express differing regulatory claims, with some focusing on safeguarding sovereignty and protecting human rights, some prioritizing economic promotion and security assurance, and others targeting traditional and innovative digital trade barriers. These varied approaches reflect the tension between three pairs of values: collectivism and individualism, freedom and security, and tradition and innovation. Based on their distinct value pursuits, three representative models of data sovereignty construction have emerged globally. At the current juncture, when international rules for digital trade are still in their nascent stages, China should timely establish its data sovereignty rules, actively participate in global data sovereignty competition, and balance its sovereignty interests with other interests. Specifically, China should explore the scope of system-acceptable digital trade barriers through free trade zones; integrate domestic and international legal frameworks to ensure the alignment of China's data governance legislation with its obligations under international trade agreements; and use the development of the "Digital Silk Road" as a starting point to prioritize the formation of digital trade rules with countries participating in the Belt and Road Initiative, promoting the Chinese solutions internationally.*

Keywords: data sovereignty ♦ cross-border data flow ♦ international trade agreements ♦ digital trade rules

The competition for resources among nations has been ongoing since the inception of nation-states. Following the rule-making seizure and resource division of physical spaces, such as land, sea, and outer space, and with the advent of the information age, countries have turned their attention to virtual space — cyberspace. Data, as an essential resource that cannot be ignored in cyberspace, has become a crucial object for countries to influence the rule-making of cyberspace. As a result, the

[*] ZHANG Qianwen (张倩雯), Professor and Master's Supervisor at the International Law School, East China University of Political Science and Law, is interested in international investment law and digital economic and trade rules. This paper is a phased result of the "Research on the Issue of China's Data Export System" (24SFB3035), a research project of the Ministry of Justice of China on the construction of the rule of law and the study of legal theories at the ministerial level in 2024.

concept of state sovereignty has expanded with new era-specific connotations, and the theory of data sovereignty has emerged in recent years. The *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* recognizes the right of states to exercise jurisdiction over data stored in their territories, but does not elaborate further on the concept of data sovereignty. There is considerable disagreement among countries as to the extent to which states can exercise sovereignty over data. While countries establish their own data sovereignty by improving their domestic data legislation, cross-border data flow poses challenges in establishing the boundaries of data sovereignty. Given that cross-border data flow is an important form of trade and investment among countries, countries, based on their respective value pursuits, are expanding their digital rule claims through bilateral and multilateral economic and trade agreements, seizing the right to make digital rules, and competing for the dominant right to delimit the boundaries of data sovereignty.

In recent years, discussions have emerged in China's academic circles regarding the connotation and nature of data sovereignty. However, the primary focus has been on data sovereignty as a prerequisite for discussion, and there is a notable lack of research on the extension of data sovereignty.[1] This paper reviews the evolution of the concept of state sovereignty from a historical perspective, and analyzes how countries construct data sovereignty through the regulation of cross-border data flow in international trade agreements, as well as the value causes and representative construction models behind it. Amid the gradual improvement of China's domestic data governance legislation, this paper aims to provide a reference for China's development of data sovereignty rules and participation in the game of international rules for digital economy and trade, thereby helping China to secure a leadership position in the international rule-making of the digital economy and trade.

I. International Law Construction of Data Sovereignty

A. Proposal of the concept of data sovereignty

The iteration of modern information and communication technologies, such as cloud computing and the Internet of Things (IoT), marks the advent of the era of big data. The cross-border flow of massive amounts of data poses a challenge to the traditional, territory-oriented concept of state sovereignty. While the volume of data has exploded, the economic benefits and strategic value of data have begun to be emphasized, with data being likened to a resource as valuable as oil.[2] A debate has arisen around whether countries enjoy data sovereignty. In fact, some scholars had put forward the concept of "data sovereignty" as early as the 1990s, which was then defined in two ways: a country enjoys state sovereignty over its data related to national security, while individuals enjoy personal "sovereignty" over their personal

---

[1] For part of the relevant studies, see Zhai Zhiyong, "The Emergency of Data Sovereignty and Its Dual Properties," *China Law Review* 6 (2018): 196-202; Zhang Xiaojun, "The Building Models of Data Sovereignty Rules and the Enlightenment: On the Rule Building of China's Data Sovereignty," *Modern Law Science* 6 (2020): 136-149; and Qi Aimin, and Zhu Gaofeng, "On the Establishment and Perfection of National Data Sovereignty System," *Journal of Soochow University (Philosophy & Social Science Edition)* 1 (2016): 83-88.

[2] Economist "The World's Most Valuable Resource is No Longer Oil, but Data," accessed May 9, 2025, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

privacy-related data.[3] The "Prism Gate" in 2013 has propelled national concerns about data sovereignty. The academic community has yet to reach a consensus on the definition of data sovereignty.[4] Most definitions emphasize the right of states and governments to control data within a country and in the cloud.[5] Among them, some scholars focus on the state's ability to protect data,[6] while others view data sovereignty as the state's power to collect and manage its data.[7] Given the greater ambiguity of the concepts of both data sovereignty and cyberspace sovereignty, there is no definitive conclusion on the relationship between data sovereignty and cyberspace sovereignty. Some scholars believe that data sovereignty is a subset of cyberspace sovereignty,[8] while others have suggested that data transmission can be realized through modern paths, such as telegraphy and remote sensing technology, and is not limited to the internet, and thus, it is not appropriate to limit data sovereignty to cyberspace.[9] Existing research shows that "cyberspace sovereignty" is commonly used in national strategies, while "data sovereignty" is often applied at the political level involving practices.[10] Although the meaning of "data sovereignty" remains controversial, the implications for a country's trade policies arising from the concept are increasingly being emphasized.[11]

The connotation of sovereignty has evolved dynamically over time. But whatever the era, there is always a fundamental commonality in the properties of sovereignty, namely, the supreme authority of a state's government within its borders and areas of jurisdiction.[12] Drawing on the traditional definition of sovereignty in international law, this paper defines data sovereignty as a state's supreme and independent control over its national data. At the same time, sovereignty is not absolute and borderless. "The time of absolute and exclusive sovereignty, however, has passed,"[13] and the authority of states and governments has boundaries.[14] The boundaries of sovereignty involve the fundamental interests of a country, and

---

[3] Joel Trachtman, "Cyberspace, Sovereignty, Jurisdiction, and Modernism," *Indiana Journal of Global Legal Studies* 5 (1998): 566.

[4] For a study concerning all literature published from August 2018 to December 2019 on "data sovereignty," see Patrik Hummel, Matthias Braun, Max Tretter and Peter Dabrock, "Data Sovereignty: A Review, Big Data & Society," available at https://doi.org/10.1177/2053951720982012.

[5] Kristina Irion, "Government Cloud Computing and National Data Sovereignty," *Policy & Internet* 4 (2012): 42-43.

[6] Sinica Alboaie, and Doina Cosovan, "Private Data System Enabling Self-sovereign Storage Managed by Executable Choreographies," *Lecture Notes in Computer Science LNCS* 10320 (2017): 86.

[7] Rainie SC, Schultz JL, Briggs E, et al. "Data as a strategic resource: Self-determination, governance, and the data challenge for indigenous nations in the United States," *International Indigenous Policy Journal*, vol. 8, no. 2 (2017): 5-6.

[8] Dana Polatin-Reuben, and Joss Wright, "An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet," USBNIX Association. Tim Maurer, et al., "Technological Sovereignty: Missing the Point?" in the *7th International Conference on Cyber Conflict: Architectures in Cyberspace*, 2015.

[9] Sun Nanxiang, and Sun Xiaojun, "On Data Security — An Examination of Game and Cooperation in Cyberspace," *Pacific Journal* 2 (2015): 64.

[10] Marie Baezner, and Patrice Robin, "Cyber sovereignty and data sovereignty," CSS Cyber Defense Project 2018, page 31.

[11] Shen Yuliang, Peng Yu, Gao Jiang, and Chen Lixing, "Digital Trade Rules or Digital Economy Rules? China's Orientation of the New Generation of Trade Rules," *Journal of Management World* 8 (2022): 68.

[12] Island of Palmas case, in Reports of International Arbitral Awards, vol. 2, 1949, page 829.

[13] The sentence is from the report that Boutros Boutros-Ghali, the sixth UN Secretary-General, submitted in 1992. See B. Boutros-Ghali, *An Agenda for Peace*, 2nd edition, New York, United Nations, 1995, page 44.

[14] Nico Schrijver, "The Changing Nature of State Sovereignty," *British Yearbook of International Law*, vol. 70, no. 1 (1999): 71.

therefore, the disputes among countries over the boundaries of sovereignty have never ceased. In the process of competing for dominance in the international regulation of the digital economy, the reasonable delimitation of data sovereignty boundaries is of great significance for a country to safeguard its state's security interests and those of its nationals, as well as to promote the development of the digital economy.

B. Construction of data sovereignty in international law

International law affects the boundaries of sovereignty. In 1923, the Permanent Court of International Justice, in the "Nationality Decrees Issued in Tunis and Morocco," stated that "The question whether a certain matter is or is not solely within the jurisdiction of a State is an essentially relative question; it depends upon the development of international relations."[15] States needed to achieve their development through international cooperation, and enabling international cooperation required compromises, i.e., ceding part of a matter of domestic jurisdiction and placing that matter within the purview of international law. Therefore, the boundaries of sovereignty are affected by international relations and remain subject to the regulation of international law. However, the extent to which sovereignty is linked to international law is influenced by international relations. In times of greater international tension, the United Nations was more reticent, and domestic jurisdictions were more likely to be interpreted broadly than in times of closer international cooperation.[16] The current trend of counter-globalization coincides with the "great changes unseen in a century." On the one hand, countries are relatively tightening their sovereignty affairs, for example, the U.S. *Foreign Investment Risk Review Modernization Act of 2018* and the *Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union* have been introduced in recent years. On the other hand, countries are actively expanding the extraterritorial influence of domestic laws by constructing an extraterritorial application system of domestic laws, and delimiting sovereign boundaries by concluding international agreements to seize the rule-making rights in emerging fields.

Digital trade is becoming an increasingly important area of international trade cooperation, encompassing the exchange of goods and services that are digitally ordered or delivered.[17] In the field of digital trade, international trade agreements are constructing data sovereignty through different models of regulating cross-border data flow. While data is as valuable as oil, it has an entirely different characteristic: data naturally flows across borders, and it is in the cross-border data flow that its significant value is realized. According to the definition of the Organization for Economic Cooperation and Development (OECD), "'transborder flows of personal data' means movements of personal data across national borders,"[18] which shows that cross-border data flow involves the boundaries of state sovereignty. Therefore,

---

[15] PCIJ, the Decrees on Nationality in Tunis and Morocco case, Series B, No. 4, 1923, page 27.
[16] Nico Schrijver, "The Changing Nature of State Sovereignty," 75.
[17] The Organization for Economic Co-operation and Development, Digital Trade, accessed May 9, 2025, https://www.oecd.org/en/topics/digital-trade.html.
[18] The Organization for Economic Co-operation and Development, Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, accessed May 9, 2025, https://legalinstruments.oecd.org/public/doc/114/114.en.pdf, page 6.

international trade agreements can construct a state's data sovereignty by regulating cross-border data flows. As a result, although states have adopted their data security legislation to establish data sovereignty, the establishment of data sovereignty can hardly be accomplished through a state's domestic legislation alone. Cross-border data flow has become a significant driving force for the development of international trade and investment, and the conclusion of international trade agreements among states to regulate cross-border data flow has also become a crucial form of constructing data sovereignty.

II. Controversial Claims and Colliding Values amid Data Sovereignty Construction

The establishment of a state's data sovereignty is far from being a mere political issue. Cross-border data flow is beneficial in promoting the development of the digital economy, yet the leakage of data may jeopardize national security and infringe on individual privacy. As a result, various propositions on data sovereignty construction exist in different countries, which involve the intersection of political, economic, cultural, and other pluralistic values.

A. Safeguarding sovereignty and protecting human rights

The relationship between sovereignty and human rights has been a subject of long-standing exploration in international jurisprudence. In this regard, there are four main types of views in the Western academic community: (a) the principle of international protection of human rights restricts state sovereignty; (b) state sovereignty hinders the protection of human rights; (c) human rights alter the connotation of sovereignty; (d) and the state has the right to decide on its own, based on the exercise of sovereignty, whether or not to accept the obligation to protect human rights.[19] Along with the introduction of national self-determination as a fundamental principle of international law, there has been an increase in the number of claims in the international community that minorities enjoy the rights to maintain their cultural integrity and freedom of religion and that the indigenous people enjoy the right to natural resources of the places and environments in which they live,[20] which constitutes a "bottom-up" challenge of human rights to sovereignty.[21] The relationship between sovereignty and human rights became the core issue of the English School of international relations theory in the 20th century, giving rise to the dispute between the "pluralism" of international society advocated by Hedley Bull, which is led by the principle of respect for sovereignty and non-interference,[22] and the "solidarism" advocated by John Vincent, which takes human rights and

---

[19] Wang Keju, "Viewpoints of Western Scholars on the Relationship Between Human Rights and Sovereignty," *Global Law Review* 3 (1997): 78-79.

[20] H. Hannum, *Autonomy, Sovereignty and Self-determination. The Accommodation of Conflicting Rights*, 2nd edition (Philadelphia: University of Pennsylvania Press, 1996); C. M. Brölmann et al. (eds.), *Peoples and Minorities in International Law* (Dordrecht: Kluwer, 1993); P. Thornberry, *International Law and the Rights of Minorities* (Clarendon: Oxford, 1991).

[21] Nico Schrijver, "The Changing Nature of State Sovereignty," 76.

[22] Hedley Bull, *The Anarchical Society: A Study of Order in World Politics*, 4th edition, translated by Zhang Xiaomiing (Shanghai: Shanghai People's Publishing House, 2015).

sovereignty as the common value for measuring the legitimacy of states.[23] The conflict between sovereignty and human rights was highlighted by NATO's military action against Kosovo in 1999, which once again triggered controversy over the legality of humanitarian intervention.[24] In the context of the trend toward the humanization of international law, it is necessary for states to reconcile the safeguarding of sovereignty with the protection of human rights. The conflict between human rights and sovereignty is also complex to avoid amid the states' data sovereignty construction through international trade agreements.

1. Protection of personal privacy

If data sovereignty falls within the realm of state sovereignty, the possible infringement of individual privacy by cross-border data flow is a challenge to data sovereignty. On the one hand, the process of data flow is accompanied by a large amount of personal privacy being collected, used, and processed. The development of electronic media, such as the internet, has profoundly transformed our daily communication habits. Mark Poster argues that the ubiquitous surveillance of people by databases is akin to a panopticon that works "continuously, systematically, and surreptitiously."[25] As a postmodern discourse, databases blur or even erase the boundaries between public and private. For example, in a scenario where a credit card is used to make a purchase, the consumer's purchasing behavior is supposed to be private. Still, when he uses the credit card to check out, it transforms the private behavior into part of the public record.[26] In a "panopticon" like a database, individuals are fully monitored and often unaware of the surveillance. Every aspect of social governance requires a substantial amount of data to support it, and individuals often have to relinquish some of their privacy, whether active or passive, leading to increased transparency.

On the other hand, cross-border data flow amplifies the risk of individual privacy protection in intra-domain data flows. Modern personal data processing technologies and business models have evolved rapidly, with personal data increasingly involved in cross-border flows. Particularly in e-commerce transactions and on social platforms, individuals can frequently initiate and control the cross-border flow of their data.[27] Technological advances have enabled individuals to gain significant economic benefits and social value from their participation in these activities, while the risk of personal data being stolen or compromised is increasing daily. The willingness, ability, and system design for personal data protection vary significantly from country to country. In the context of cross-border data flow, there are frequent incidents of personal data leakage resulting from attacks initiated by criminals or hackers. In March 2018, a large amount of personal data of Facebook users was posted to a hacker forum in the U.S., which included phone numbers, Facebook login IDs, full

---

[23] John Vincent, "Grotius, Human Rights, and Intervention," in *Hugo Grotius and International Relations*, Hedley Bull, Benedict Kingsbury, and Adam Roberts eds. (Oxford: Oxford University Press,1992), 242.

[24] Luo Guoqiang, "The International Law Theories of 'Humanitarian Intervention' and Their Latest Development," *Law Science* 11 (2006): 86-91.

[25] Mark Poster, *The Second Media Age*, translated by Fan Jinghua (Nanjing: Nanjing University Press, 2000), 120.

[26] Ibid., 121-122.

[27] Christopher Kuner, "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future," *OECD Digital Economy Papers* 187 (2011): 11.

names, addresses, dates of birth, resumes, and email addresses, related to 533 million Facebook users from 106 countries. The data was later jointly disclosed by *The New York Times* and *The Observer* in the UK as having been illegally collected by Cambridge Analytica for use in the U.S. presidential election by the Trump administration.[28] It can be seen that there is a greater risk to personal privacy protection in cross-border data flows. If countries enjoy data sovereignty requiring the free flow of data across borders, the protection of individual privacy will affect the boundaries of data sovereignty.

2. Preservation of indigenous cultures

As one of the manifestations of globalization, cross-border data flow naturally brings with it the adverse effects of globalization, namely, the dissolution of the original identity of countries and regions,[29] with particular impact on indigenous cultures. To guarantee the right of indigenous peoples to maintain their institutions, cultures, and traditions, the United Nations Economic and Social Council established the United Nations Permanent Forum on Indigenous Issues in 2000. Actions such as collecting, processing, and monitoring data require significant financial resources, while indigenous peoples are generally economically disadvantaged and therefore lack sufficient data governance capacities.[30] Given this, improving the data collection and processing capacity of indigenous peoples was listed on the agenda of the United Nations Statistics Division.[31] Based on the purposes of the *Charter of the United Nations*, the United Nations adopted an essential human rights treaty of human rights in 2007, namely the *United Nations Declaration on the Rights of Indigenous Peoples*, the preamble of which states that we should "respect and promote the inherent rights of indigenous peoples which derive from their political, economic and social structures and their cultures, spiritual traditions, histories and philosophies, especially their rights to their lands, territories and resources." In the information age, cross-border data flow is a double-edged sword for indigenous peoples: it facilitates the provision of a wide range of information for indigenous peoples' development, helping them to allocate resources, make decisions and influence public opinion; at the same time, however, cross-border data flow can have an impact on indigenous cultures, rights, and intellectual property rights, and may constitute a dismantling of state sovereignty, especially in the case of a state that is predominantly indigenous.[32] The term "indigenous data sovereignty" was thus coined to emphasize the fundamental right of indigenous peoples to protect their cultural identity and promote their well-being in the context of data governance, which is at the heart of realizing

---

[28] The Guardian: Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, accessed May 9, 2025, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

[29] Christopher Kuner, "Data nationalism and its discontents," *Emory Law Journal Online* 64 (2015): 2092, available at http://law.emory.edu/elj/elj-online/volume-64/responses/data-nationalism-its-discontents.html.

[30] C Matthew Snipp, "What does data sovereignty imply: what does it look like?" in *Indigenous Data Sovereignty: Toward an Agenda*, Tahu Kukutai and John Taylor ed. (Canberra: ANU Press, 2016), 40.

[31] Report of the Workshop on Data Collection and Disaggregation for Indigenous Peoples, United Nations Doc. E/C. 19/2004/2 [11].

[32] Diane E Smith, "Governing data and data for governance: the everyday practice of indigenous sovereignty," in *Indigenous Data Sovereignty: Toward an Agenda*, Tahu Kukutai and John Taylor ed. (Canberra: ANU Press, 2016), 131-132.

the national right to self-determination, a fundamental principle of international law.[33] The appropriate restriction on the impact and even erosion of cross-border data flows on indigenous peoples' native cultures is one purpose that should not be overlooked amid the construction of data sovereignty.

B. Promoting the economy and ensuring security

There had been controversy within the World Trade Organization (WTO) regarding whether digital trade constituted trade in services or trade in goods;[34] however, it was considered a form of trade in either case. Digitization has transformed the scope, scale, and speed of international trade, contributing significantly to its growth.[35] Cross-border data flow, on the other hand, is the foundation of digital trade and lies at the heart of rapidly growing emerging models of service supply, such as cloud computing, the IoT, and additive manufacturing. Additionally, cross-border data flow promotes the implementation of trade facilitation measures and indirectly contributes to the growth of trade.[36] A 2018 study by the OECD showed that for every 10 percent increase in bilateral digital connectivity between countries, trade in goods between countries can increase nearly twofold.[37]

The free flow of data across borders not only promotes the growth of international trade but also contributes to international investment. The growth of the digital economy has opened doors for small and medium-sized investment businesses in particular. At one time, businesses needed to grow to a significant size before they could afford the resources needed to export. Still, digitization has dramatically reduced the minimum size required to run a cross-border business, allowing even small and medium-sized enterprises (SMEs) to link up with consumers and suppliers worldwide easily.[38] Cross-border data flow enables SMEs to access information technology (IT) services and reduce their upfront investment costs in digital infrastructure. Based on the optimization of access to core knowledge and key information capabilities, SMEs can overcome their original information accessibility shortages and gain the opportunities to compete with larger competitors.[39] Thus, by removing information barriers, cross-border data flow empowers SMEs to link globally, creating an emerging variety of "micro-multinational enterprises" that are inherently global.[40] On the contrary, if the free flow of data across borders is restricted, the negative economic impact on SMEs is more pronounced than on large multinational enterprises.[41]

While enhancing the economic efficiency of trade and investment, the cross-border data flow has also created new security risks involving national security

---

[33] Ibid., 132.
[34] Magnus Lodefalk, "The Role of Services for Manufacturing Firm Exports," *Review of World Economics* 150 (2014): 71.
[35] López González, J. and J. Ferencz, "Digital Trade and Market Openness," *OECD Trade Policy Papers* 217 (2018):10-11, available at http://dx.doi.org/10.1787/1bd89c9a-en.
[36] López González, J. and M. Jouanjean, "Digital Trade: Developing a Framework for Analysis," *OECD Trade Policy Papers* 205 (2017): 10, available at https://doi.org/10.1787/524c8c83-en.
[37] López González, J. and J. Ferencz, "Digital Trade and Market Openness," 24.
[38] James Manyika, et al., "Digital globalization: the new era of global flows," MGI, 2016, page 43.
[39] Casalini, F. and J. López González, "Trade and Cross-border Data Flows," *OECD Trade Policy Papers* 220 (2019): 14, available at https://doi.org/10.1787/b2023a47-en.
[40] James Manyika, et al., "Digital globalization: the new era of global flows," MGI, 2016, page 44.
[41] Anupam Chander, and Uyên P. Lê, "Data Nationalism," *Emory Law Journal* 64, no. 3 (2015): 722.

and public safety, such as cybersecurity and financial security.[42] The exposure of the "Prism Program" in June 2013 revealed the U.S. National Security Agency's secret six-year-long electronic eavesdropping program, whose targets included a large number of citizens of countries other than the U.S., which has made countries realize the importance of safeguarding the security of cross-border data flow for national interests. In April 2008, HSBC lost an unencrypted disk containing the life insurance information of 370,000 customers, including their names, dates of birth, policy numbers, amounts insured, and smoking habits.[43] In April 2018, HSBC's financial systems were attacked again, and some customer data was stolen. Financial data has become a frequent target of cyberattacks in recent years due to its significant economic value, making it imperative to safeguard financial security in cross-border data flows. Based on the specific scenario of cross-border data flows, the security involved encompasses both "static security," such as maintaining the integrity, availability, and confidentiality of data, and "dynamic security," which ensures the control of both critical and non-critical data throughout the data flow process.[44] In this regard, the static security of data is a prerequisite for the free flow of data across borders, and the dynamic security of data is a hard and soft constraint that enables data to flow freely.[45] As a result, safeguarding security while promoting the digital economy is a crucial consideration for countries to regulate cross-border data flows.

C. Traditional and new barriers

From the perspective of global governance, international law exhibits a distinctive dynamic nature, which requires both tradition and continuous innovation, presenting a dialectical relationship of opposites and unity.[46] Cross-border data flow, as a new topic in the era of big data, also reflects the tradition and innovation of international law. Reasonable regulation of cross-border data flows requires not only compliance with the fundamental laws and intrinsic values of international law, but also the release of the creativity of international law to promote the birth of international rules that are responsive to the needs of the times.

The dialectical relationship is particularly reflected in the recognition of digital trade barriers. The OECD conducts an annual review of digital trade barriers, whose variety has grown in line with the times. As mentioned earlier, cross-border data flow can help facilitate international trade, but the commitments made in the 1994 Uruguay Round negotiations of the WTO did not specifically refer to e-commerce and data flows.[47] In 1998, the members of the WTO adopted the *Declaration on Global*

---

[42] For policy considerations of countries during the legislation process on cross-border data flow, see Zhang Qianwen, "Regulation of the IIA Exception Clause for Cross-border Data Flows," *Law Science* 5 (2021): 93.

[43] The Guardian: HSBC loses disk with policy details of 370,000 customers, accessed May 9, 2025, https://www.theguardian.com/business/2008/apr/08/hsbcholdingsbusiness.banking.

[44] Xu Ke, "Freedom and Security: The China Plan for Cross-border Data Flow," *Global Law Review* 1 (2021): 32-33.

[45] Ibid., 33-35.

[46] Zhao Jun, "Innovation on the Basis of Past Achievements in International Law: From the Perspective of the Regulatory Demands of the Reform of the Global Governance System," *Chinese Social Sciences Net* 5 (2021): 26-50.

[47] However, the *General Agreement on Trade in Services* (GATS), the *General Agreement on Trade in Goods*, and the *Agreement on Trade-Related Aspects of Intellectual Property Rights* (TRIPS) all deal with issues related to electronic commerce to varying degrees. For example, the GATS categorizes trade in services into four modes, all of which are relevant to electronic commerce.

Electronic Commerce at the second session of the WTO's Ministerial Conference in Switzerland, which led to the establishment of the WTO Work Programme on E-Commerce to study issues related to electronic commerce and data flows.[48] In December 2017, the members of the WTO issued a *Joint Statement on Electronic Commerce* at the 11th session of the WTO's Ministerial Conference in Argentina and launched "negotiations on trade-related aspects of electronic commerce."[49] In January 2019, 76 members of the WTO signed the *Joint Statement on Electronic Commerce*, officially launching negotiations on the trade-related aspects of e-commerce.[50] The "non-papers" submitted by members of the WTO since 2016 have gradually begun to address the regulation of digital trade barriers. For example, Brazil proposed that the WTO should support online transactional services, including data flows, under Mode 1 of the *General Agreement on Trade in Services* (GATS). The U.S. proposed that data localization should be prohibited and that limitations should be imposed on the protection of consumer data when it flows across borders in compliance with the exception.[51]

From the 1990s, when digital trade barriers were not yet covered by international trade agreements, to the present-day debate on personal information protection, data localization requirements, source code fulfillment requirements and other barriers, it can be seen that the world's understanding of digital trade barriers is a constantly evolving process, and that in the future there will surely be more new types of barriers to be included in the scope of national attention and regulation. If all requirements that would have a limiting effect on the free flow of data across borders are considered as barriers, there are four broad types of barriers: discriminatory treatment barriers represented by restrictions on foreign investment, data localization barriers represented by requirements for localized storage of data, technological barriers represented by restrictions on or prohibitions on the use of encryption technologies, and other barriers such as weak intellectual property protection, restrictions on online advertising, and disinformation.[52] However, a lack of consensus remains among countries on which barriers distort international trade and which barriers countries have the right to regulate,[53] significantly hindering the process of formulating multilateral rules for the digital economy and trade.

D. Analysis of the impact of disputed claims on data sovereignty construction

Each of the above three sets of controversial claims reflects different value orientations and can have a limiting or expanding effect on the boundaries of data sovereignty (see Table 1). Emphasizing data sovereignty in the controversy between the preservation of sovereignty and the protection of human rights reflects the pursuit of collectivism and the relative expansion of the boundaries of data sovereignty; whereas, in the view of the theory of individualism, the state sovereignty derives from

---

[48] "WTO Work Programme on E-Commerce" (n 1) adopted on September 25, 1998.
[49] "WTO Work Programme on E-Commerce: Ministerial Decision of December 13, 2017" (WTO 2017) Ministerial Conference Eleventh Session WT/MIN(17)/65; WT/L/1032.
[50] WTO, Joint Statement on E-commerce, WT/L/1056, January 25, 2020.
[51] Nivedita Sen, "Understanding the Role of WTO in International Data Flows: Taking the Liberalization or the Regulatory Autonomy Path?" *Journal of International Economic Law* 2 (2018): 339-341.
[52] Susan Ariel Aaronson, "The Difficult Past and Troubled Future of Digital Protectionism," in *Addressing Impediments to Digital Trade*, Ingo Borchert and L Alan Winters eds. (London: CEPR Press, 2021), 144.
[53] Ibid., 146.

the cession of the rights of the individual, and the power of the state can be reduced to the rights of the individual.[54] Therefore, both the protection of individual privacy and the protection of indigenous peoples' native cultures are intended to comply with the values of individualism and respect for the fundamental rights and will of the human being as an individual. The guarantee of individual human rights, on the other hand, would relatively limit the boundaries of national data sovereignty. In the contested claims of economic promotion and security protection, the proposition that the free flow of data across borders promotes economic and trade development reflects the values of liberalism. Classical liberal economics and neoclassical liberal economics both center on the free market, although they differ in their understanding of the market's nature.[55] The free flow of data across borders, if allowed, would help facilitate international trade, but would also limit the boundaries within which states could exercise data sovereignty. On the contrary, if security interests, such as safeguarding national security, cybersecurity, and financial security, are prioritized, states will be more proactive in exercising their sovereign power and thus tend to expand the boundaries of data sovereignty. In the battle between traditional and new barriers to digital trade, countries are currently focusing more on traditional forms of barriers; however, new types of barriers are likely to receive more attention in the future. If more new types of barriers are regulated, cross-border data flow will move toward greater liberalization, and the boundaries of data sovereignty will be relatively constricted compared to adherence to traditional barriers.

Table 1 Impact of Value Collisions on Data Sovereignty Construction

Effect	Boundary restriction			Boundary expansion		
Proposition	Protection of human rights	Promotion of the economy	New barriers	Preserving sovereignty	Safeguarding security	Traditional barriers
Value	Individualism	Freedom	Innovation	Collectivism	Security	Tradition

Therefore, the different claims of states in constructing data sovereignty reflect different value pursuits, which have been reflected in the domestic laws of various states. The claims of U.S. foreign digital trade policies are mainly embodied in the *Digital 2 Dozen*. Leveraging its strengths in the IT industry, the U.S. upholds a "freedom-first" approach and promotes a market-driven model that facilitates cross-border data flows as a fundamental principle.[56] The EU regards the right to data as a fundamental human right and restricts the cross-border flow of personal data following the *General Data Protection Regulation* (GDPR). China's regulations of cross-border data flows are based on the *Cybersecurity Law,* the *Data Security Law, and* the *Personal Information Protection Law*, which emphasize information security and promote the orderly flow of data across borders. Considering these widely differing claims and value orientations, after establishing data sovereignty through domestic laws, countries have further engaged in games and compromises in the

---

[54] H. Steiner, "Territorial Justice and Global Redistribution," in *The Political Philosophy of Cosmopolitanism*, G. Brock and H. Brighouse eds. (Cambridge: Cambridge University Press, 2005), 33.

[55] For the understanding of neoclassical liberal economics on the nature of free market, see Yang Chunxue, "The Dilemma of Neoliberalism Economics and a Critique," *Economic Research Journal* 10 (2018): 6-8.

[56] *The Digital-2-Dozen*, accessed May 9, 2025, https://ustr.gov/sites/default/files/Digital-2-Dozen-Final.pdf.

negotiation of international trade agreements, forming different models of data sovereignty construction.

III. Main Models for Data Sovereignty Construction in International Trade Agreements

A. Data sovereignty contraction model driven by economic efficiency

Liberalism dominates the American political tradition, and the modern American state system is based on liberal principles and values.[57] The path of the U.S.'s data sovereignty construction in the international trade agreements it has concluded follows its liberal tradition. As mentioned earlier, numerous prior studies have demonstrated that the free flow of data across borders facilitates international trade and investment. Conversely, restricting the free flow of data across borders increases costs for businesses.[58] Given this, the international trade agreements concluded by the U.S. prioritize the promotion of economic and trade development as their primary objective and have established a data sovereignty contraction model driven by economic efficiency.

The *Comprehensive and Progressive Agreement for Trans-Pacific Partnership* (hereinafter referred to as "TPP"), formed under the leadership of the U.S., embodies the U.S. attitude of promoting the free flow of cross-border data in the U.S. *Digital 2 Dozen*. Although there are still some ambiguities in the wording of TPP, it is nonetheless seen as a milestone in international rules for the digital economy.[59] Even though the U.S. has withdrawn from the TPP, it continues implementing the entirety of the e-commerce chapter of the original agreement, including provisions on cross-border data flow. Article 14.11 of the TPP outlines the basic principles for the free flow of data across borders, with exceptions to protect legitimate public policy objectives. Article 14.13 prohibits, in principle, local data storage requirements and only allows member states to adopt measures that are necessary, non-discriminatory, and non-trade-restrictive to "achieve a legitimate public policy objective." Concerning the protection of personal information, Article 14.8 of TPP states that "each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce." In particular, a Party may "adopt or maintain measures 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" to exercise their obligations of personal information protection. However, Article 14.8 chose to use the wordings of "may," which is milder and considered more "on principle" compared to "no party shall" used in articles to prohibit data localization.

This model was further elaborated in the *United States-Mexico-Canada Agreement* (USMCA). The predecessor to the USMCA, the *North American Free*

---

[57] For studies on liberalism in the U.S., see Qian Mansu, *American Liberalism and Its Transformation* (Beijing: SDX Joint Publishing Company, 2006).

[58] e.g. Swedish Board of Commerce, "No transfer, no production — a report on cross-border data transfers, global value chains and the production of goods," European Commission, April 28, 2015, accessed May 9, 2025, https://ec.europa.eu/futurium/en/system/files/ged/publ-no-transfer-no-production.pdf.

[59] Neha Mishra, "The Role of the Trans-Pacific Partnership Agreement in the Internet Ecosystem: Uneasy Liaison or Synergistic Alliance?" *Journal of International Economic Law* 20, no. 1 (2017): 38-39.

Trade Agreement (NAFTA), was limited by the era in which it was concluded and did not address specialized rules for the digital economy and trade. The USMAC, reached in November 2018, further strengthens the principle of facilitating the free flow of data across borders, building on the TPP, by setting forth standards for personal information protection among the contracting parties and removing the exception to the localization of facilities requirement in Article 14.13 of the TPP.[60] The USMAC also applies the prohibition of localization requirements to the financial services sector in Articles 17.17 and 17.18 in the Financial Services Chapter. Given the strength of U.S. digital businesses in the computer and communications sector, the USMAC specifically adds a protection clause for algorithms to TPP's source code protection provision, limiting the governments' authority to require disclosure of source code and algorithms.[61] Article 19.17 of the USMCA also limits the liability of Internet Service Providers (ISPs) by clarifying that they shall not be liable for infringements resulting from a user's transmission of information on that platform. Overall, the USMCA is more stringent and comprehensive than the TPP in terms of facilitating the free flow of data across borders. In addition to multilateral treaties, the *U.S.-Japan Digital Trade Agreement* (USJDTA) reached in 2019 follows the USMCA's provisions relating to the prohibition of data localization, the promotion of the free flow of data across borders, and the protection of source code.

Observing the relevant provisions of the TPP, the USMCA, and the USJDTA on cross-border data flow, it can be seen that freedom-oriented economic efficiency is the primary value choice of the U.S. in constructing data sovereignty. For this reason, the e-commerce chapter of the TPP does not include the exceptions of essential security interest, national security, public morals, and public order, which are commonly found in international trade agreements, but only provide for the right of member states to protect their own legitimate public policy objectives, subject to specified conditions, in Articles 14.11 and 14.13. The USMCA even removes the legitimate public policy objective exception and adds more provisions that help promote economic efficiency, such as the algorithmic protection provision. In addition, the TPP and the USMAC contain more principled provisions on the protection of personal information, while the prohibition of data localization is more stringent and specific. Therefore, it can be concluded from these treaties that the need to safeguard security interests and protect individual privacy has given way to the need to promote economic efficiency as a subsidiary value. It is worth noting that the *Digital Economy Partnership Agreement* (DEPA), concluded in June 2020, contains many similar rules for cross-border data flow to those in the TPP; however, the former builds on the latter with refinements.[62] The U.S. is not a member of the DEPA, but the parties to the DEPA are all members of the TPP. This may suggest that freedom-oriented economic efficiency is also a primary concern for the members of the DEPA. However, if economic efficiency is to be used as a measure of legal rules, a precondition should be met: economic efficiency

---

[60] USMCA, Art. 19.8, Art. 19.12.
[61] USMCA, Art. 19.16.
[62] Zhao Yangdi and Peng Delei, "Latest Development and Comparison of Global Digital Economy and Trade Rules Based on the Study of the Digital Economy Partnership Agreement," *Asia-Pacific Economic Review* 4 (2020): 63.

is desirable in itself and is prioritized over other values.[63] The pursuit of economic efficiency by the U.S. stems from the absolute advantage of its science and technology enterprises themselves; however, such technological strength does not exist in many other countries, and thus, its pursuit of economic efficiency is difficult to gain the approval of most countries.

B. Digital sovereignty contraction model led by human rights protection

Unlike the U.S., the EU takes a more cautious approach to the free flow of data across borders. During World War II, the personal information of a large number of Jews was compromised, which led directly to them being targeted for capture and slaughter by the Nazis. Considering the lessons learned from the two world wars, the EU has placed special emphasis on the protection of human rights and has included data protection as a fundamental human right. Paragraph 1 of Article 8 (Protection of personal data) of the *Charter of Fundamental Rights of the European Union* states that "Everyone has the right to the protection of personal data concerning him or her."[64] Likewise, Article 8 of the EU's *Convention for the Protection of Human Rights and Fundamental Freedoms* also establishes the right to privacy as an essential element of fundamental human rights in Paragraph 1: "Everyone has the right to respect for his private and family life, his home and his correspondence."[65]

Guided by the idea of treating personal data as a fundamental human right, the EU is an early global leader in legislation for the protection of personal data.[66] In 1981, the Council of Europe adopted the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, which establishes harmonized rules and standards for the protection of personal data on a European scale through legislative means.[67] In 1995, the EU adopted the *Directive 95/46/EC of the European Parliament and of the Council 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*, which restricts cross-border data transfers from EU member states to non-member States, introducing the principle that the country of destination of the data transfer must have the capacity to provide adequate protection of data, as recognized by the European Commission.[68] To further strengthen the comprehensive protection of personal data, the EU GDPR came into force in 2018, reflecting the EU's desire to establish a "digital single market."[69] Paragraph 2 of Article 1 in the GDPR states that "This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data." Accordingly, the GDPR

---

[63] Arthur Allen Leff, "Economic Analysis of the Law: Some Realism About Nominalism," *Virginia Law Review* 60 (1974): 464-465. This paper is a book review of Richard A. Posner's *Economic Analysis of Law* published in 1973.

[64] *Charter of Fundamental Rights of the European Union*, 2000 O. J C 364/10.

[65] *Convention for the Protection of Human Rights and Fundamental Freedoms*, November 4, 1950, 312 U.N.T.S. 222, Art. 8.

[66] Paul M. Schwartz, "European Data Protection Law and Restrictions on International Data Flows," *Iowa Law Review* 80, no. 3 (1994): 471.

[67] *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, European Treaty Series, No.108.

[68] *Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Official Journal L 281, 23/11/1995 P. 0031-0050. Art. 25.

[69] Huang Ning and Li Yang, "The Evolutionary Trend of Trans-border Data Flows Regulation and Its Cause Analysis," *Journal of Tsinghua University (Philosophy and Social Sciences)* 5 (2017): 175.

regulates the collection and use of personal data, as well as the rights of data subjects. In addition to confirming the original "principle of full protection," it also grants data subjects essential rights such as the right to consent, the right to access, the right to portability, the right to be forgotten, and the right to rectification, and puts forward the principle of data minimization and other principles, which more strictly restrict the cross-border flow of personal data. In addition, the GDPR sets severe penalties for processing data in violation of the law and has discouraged some digital businesses from investing in the EU due to its strong extraterritorial effect.

Based on the harmonization of data protection legislation within the EU, the EU has subsequently promoted its data protection claims in bilateral agreements. Unlike the TPP and the USMCA outlining in principle the obligations of the contracting parties to protect personal information, in contrast, the EU typically sets out, in detail, the obligations of the contracting parties to protect personal information in the e-commerce chapters of its bilateral economic and trade agreements. For example, the *EU-Singapore Investment Protection Agreement* explicitly provides for "the protection of the privacy of individuals in relation to the processing and dissemination of personal data" and "the protection of confidential of individual records and accounts" in the paragraph under Article 2.3 (National Treatment).[70] The *EU-South Korea Free Trade Agreement* first emphasizes that "development of electronic commerce must be fully compatible with the international standards of data protection" in Article 7.48(2), which sets out the object and purpose, and then goes on to propose five issues for regulatory cooperation, including "the protection of consumers in the ambit of electronic commerce," in Article 7.49; it also includes the personal privacy protection as an exception in the e-commerce chapter.[71] In the *EU-Vietnam Free Trade Agreement* (EVFTA), data protection is no longer placed in the chapter on e-commerce, but is included in Article 8.53 "general exceptions" as a form of exception.[72] The EVFTA elevates data protection above a mere exception to the e-commerce chapter. The *EU-Canada Comprehensive Economic and Trade Agreement* (CETA) reaffirms the "adequate safeguards to protect privacy" stated in the GDPR and strictly requires that "each party shall maintain adequate safeguards to protect privacy, in particular with regard to the transfer of personal information,"[73] and, similarly to the EVFTA, includes the protection of personal privacy in the "general exceptions."[74]

However, in recent years, some of the bilateral economic and trade agreements concluded by the EU no longer emphasize only human rights protection, but have begun to include digital economic and trade clauses aimed at promoting economic development, the most representative of which is the *EU-Japan Economic Partnership Agreement* (EJEPA). In contrast to the bilateral economic and trade

---

[70] *Investment Protection Agreement Between the European Union and Its Member States, of the One Part, and the Republic of Singapore, of the Other Part*, 2018, Art. 2.3.3 (e).
[71] *Free Trade Agreement Between the European Union and Its Member States, of the One Part, and the Republic of Korea, of the Other Part*, 2010, Art. 7.48, 7.49 and 7.50.
[72] *Free Trade Agreement Between the European Union and the Socialist Republic of Vietnam*, 2018, Section G — Art. 8.53 (i. ii.).
[73] CETA, cit., Ch. 13, Art. 13.15, para. 2.
[74] Ibid, cit., Ch. 13, Art. 28.3.2 (c).

agreements mentioned above, which the EU has concluded, the digital trade provisions of the EJEPA are considered a substantial step forward.[75] Among all the bilateral economic and trade agreements concluded by the EU, Article 8.73 of the EJEPA introduces the principle that "a party may not require the transfer of, or access to, source code of software owned by a person of the other party." Another breakthrough of the EJEPA was the introduction, for the first time, of a provision stating that "the parties shall reassess within three years of the date of entry into force of this Agreement the need for inclusion of provisions on the free flow of data into this Agreement."[76] Although the provision sidesteps the question of how it will be concretely implemented, it shows the EU's efforts toward more unrestricted cross-border data flow. In contrast, the upgraded *EU-Mexico Free Trade Agreement* is the first trade agreement concluded by the EU to use the term "digital trade" in place of the previous term "electronic commerce" (e-commerce).[77] Like some of the EU's most recent bilateral economic and trade agreements, the *EU-Mexico Free Trade Agreement* sets out in its opening Article 1 the two primary purposes of the agreement: to promote economic development and to safeguard the regulatory powers of the contracting parties. In the context of guaranteeing the regulatory rights, it is crucial to ensure that parties' powers of social and consumer protection, privacy and data protection, and the promotion of the protection of cultural diversity. The *EU-Mexico Free Trade Agreement* follows the provisions of the EJEPA regarding the reassessment within three years of the inclusion of free flow of data provisions and the prohibition of mandatory disclosure of source codes.

From the bilateral trade agreements concluded by the EU, it can be seen that the EU has consistently emphasized the digital sovereignty contraction model, led by human rights protection, in which particular attention is paid to standardizing personal privacy protection to align with the GDPR. However, the *EU-Mexico Free Trade Agreement* and the EJEPA, concluded in recent years, show that the EU has begun to pay attention to the realization of economic development values while upholding the values of human rights protection. As a result, these agreements have begun to explore the incorporation of provisions to promote the free flow of data across borders, aiming to reduce barriers to digital trade, such as the mandatory disclosure of source codes. Some EU member states have also drawn the European Commission's close attention to the need to include provisions on cross-border data flow in trade agreements.[78] The EU is currently negotiating free trade agreements with Chile, Indonesia, and New Zealand. It is foreseeable that the EU will likely continue exploring the inclusion of provisions to facilitate the free flow of data across borders in future bilateral economic and trade agreements. However, due to the inherent conflict between the free flow of data across borders and the goal of protecting

---

[75] Jan A. Micallef, "Digital Trade in EU FTAs: Are EU FTAs Allowing Cross Border Digital Trade to Reach Its Full Potential?," *Journal of World Trade* 53, no. 5 (2019): 860.

[76] *Agreement Between the European Union and Japan for An Economic Partnership*, 2018, Art. 8.81.

[77] Jan A. Micallef, "Digital Trade in EU FTAs: Are EU FTAs Allowing Cross Border Digital Trade to Reach Its Full Potential?," 862.

[78] Letter on data flows to the Vice-President of the European Commission, Frans Timmermans, by ministers of like-minded member states, dated May 15, 2017, accessed May 9, 2025, https://www.politico.eu/wp-content/uploads/2017/05/POLITICO_joint-letter-eu-countries-data-flows-in-trade_May-15-2017.pdf.

individual privacy, the pursuit of economic development will still yield to the pursuit of human rights protection in a secondary position.

C. Data sovereignty expansion model driven by pluralistic value orientations

In the context of building a community with a shared future for humanity, human rights and sovereignty are, in fact, in a dialectical unity, and the protection of human rights should be based on respect for sovereignty.[79] The same applies to building a community with a shared future in cyberspace, in which the unity among safeguarding data sovereignty, protecting human rights, and ensuring security should be addressed appropriately. The *Regional Comprehensive Economic Partnership Agreement* (RCEP), concluded in 2020, could serve as a model that considers multiple values.

The RCEP comprehensively reflects the balance between safeguarding national data sovereignty and promoting economic development and security interests in its Chapter 12 (Electronic Commerce). Article 14 of this chapter, while first recognizing the need of Parties for diversity in the use or location of computing facilities, provides that parties may not, in principle, require a covered person to use or locate computing facilities as a condition for conducting business, but at the same time provides for legitimate exceptions for Parties to achieve "a legitimate public policy objective" and protect their "essential security interests," and emphasizes that "the necessity behind the implementation of such legitimate public policy shall be decided by the implementing Party," which elaborates the self-adjudicatory nature of the provision. Regarding provisions such as the prohibition on localizing facilities, and to fully respect the data sovereignty of the parties, the agreement also grants sufficient transitional periods to countries like Cambodia and the Lao PDR. Article 12.15 also begins by emphasizing that "each Party may have its own regulatory requirements concerning the transfer of information by electronic means." On this basis, the article, in principle, allows for the free flow of data across borders for business purposes, with the same exceptions for "legitimate public policy objectives" and "essential security interests." In addition, Article 12.8 requires parties to "adopt or maintain a legal framework which ensures the protection of personal information of the users of electronic commerce," and "publish information on … how individuals can pursue remedies and businesses can comply with any legal requirements." Compared with the "adequacy" requirements for cross-border transfers of personal data in the bilateral economic and trade agreements concluded by the EU mentioned above, the provisions of the RECP on the protection of personal data are more principled, and the standards are more lenient.

The regulatory provisions on cross-border data flow in the RCEP are characterized by two key aspects. First, "pluralistic values." Because of the large number of member states, the agreement does not emphasize a single value, but instead seeks to strike a balance between multiple values, which also reflects a path toward building a community with a shared future for humanity. The RCEP both affirms the importance of economic development by including provisions that prohibit

---

[79] Liao Fan, "The Implication of Human Rights and Sovereignty in the Context of the Community of a Shared Future for Mankind," *Jilin University Journal (Social Sciences Edition)* 6 (2018): 31-33.

the localization of facilities and ensure the free flow of data across borders, premised on commercial practices, and requires parties to make efforts to protect personal information from a human rights perspective. In addition, the agreement recognizes the respective regulatory needs of the parties and safeguards the data sovereignty and security interests of the parties through provisions such as "legitimate public policy objectives," "essential security interests" and self-adjudication clauses, which expresses the pursuit by the contracting parties of the diversified values of promoting the economy, protecting human rights, safeguarding sovereignty, and ensuring security. Second, "expansion of sovereignty." While the RCEP reflects the parties' pursuit of pluralistic values, its emphasis on the parties' respective regulatory requirements, the setting of preconditions for cross-border data flow and prohibition of localization, as well as the series of exception clauses, self-adjudication clauses, and transition periods, and the principled descriptions of the protection of personal information, reflect that the parties continue placing data sovereignty at the top of their priorities, which is consistent with the China's data governance model, which has always emphasized national censorship and prioritization of security.[80] Overall, the e-commerce provisions of the RCEP are still limited to regulating data in the traditional area of e-commerce and do not break new ground in the relevant content of bilateral economic and trade agreements that China has concluded in the past.[81] However, the agreement differs significantly from the "American template" and the "European template" of digital trade rules, representing the emergence of a model for data sovereignty expansion under the direction of multiple values.

IV. China's Position and Choices for Constructing Data Sovereignty Rules in International Trade Agreements

A. Necessity of constructing data sovereignty rules

The *Resolution of the Central Committee of the Communist Party of China on Further Deepening Reform Comprehensively to Advance Chinese Modernization* states that we will "boost our governance and regulatory capabilities in relation to data security and put in place a mechanism to ensure efficient, convenient, and safe cross-border data flows" and "participate in the formulation of international rules." The development of rules for the digital economy and trade has become a significant concern in the negotiation of international trade agreements. China is actively striving for stronger rights of speech in the formulation of international trade rules, paying close attention to the construction of digital trade rules, and has recently applied for accession to the TPP and the DEPA, which require it to actively benchmark against the high standards set out in those agreements. In joining the TPP, China will be directly confronted with a game against the data sovereignty contraction model driven by economic efficiency. In view of this, China should, on the basis of safeguarding

---

[80] For comments on data governance models in the U.S., EU, and China, see Susan A. Aaronson, and Patrick Leblond, "Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO," *Journal of International Economic Law* 21, no. 2 (2018): 245-272.

[81] Peng Yue, "Digital Trade Governance and Its Regulatory Approaches," *Journal of Comparative Law* 4 (2021): 166.

data sovereignty, reasonably regulate cross-border data flows and actively promote the development of digital trade. It is thus necessary to prudently consider the construction of data sovereignty rules in international trade agreements.

China has consistently adhered to the fundamental principles of security and development in governing cyberspace, and this should also be our stance in shaping the rules governing cyberspace. China is not only a host country for foreign digital enterprises' investments, but also a home country for outbound investments by Chinese digital enterprises. As a significant source of data, China should pay close attention to the issue of data protection, i.e., adherence to the principle of security. At the same time, as a large country with significant foreign digital investment, China has an interest in promoting the free flow of data across borders, that is, adhering to the principle of development. However, the philosophy of data regulation reflected in the international trade agreements concluded by China can be summarized as "security first, limited development," which emphasizes more on the data sovereignty of the contracting parties and not much on the promotion of cross-border data flow, indicating a feature of "state-centrism" over "liberalism," which is not conducive to tapping the development potential of digital enterprises in China. In the future of global governance, the tug-of-war between "state-centrism," which emphasizes the power of the state, and "liberalism," which pursues individual interests, will continue existing.[82] In the short term, state-centrism may become more pronounced in the current context of geopolitical complexity; however, liberalism may prevail in the long-term battle against state-centrism, especially in the current age of the internet and information technologies characterized by digitalization.[83] Therefore, adapting to the characteristics of the times and fully leveraging our technological advantages are key factors that should be considered when China constructs data sovereignty in international trade agreements.

B. Feasibility of constructing data sovereignty rules

In terms of feasibility, the difficulty in establishing rules for data sovereignty lies mainly in reaching a consensus between China's regulatory model and the regulatory models of other states during negotiations on international trade agreements. Behind regulatory claims are value choices. The divergence of states' data regulation propositions reflects the differences in their value choices, which directly lead to the difficulties in reaching multilateral international rules on the digital economy and trade, due to the following reasons: first, the different essence of the three regulation models. For the pluralistic-valued model, although it takes into account a variety of values, both economic efficiency and human rights protection need to give way to data sovereignty (for security interests), and therefore, the pluralistic-valued model is a data sovereignty expansion model, while the models adopted by Europe and the U.S. are all data sovereignty contraction models. Second, different value priorities. The pluralistic-valued model is a model that balances interests with a priority on security. In contrast, the economic efficiency-driven model can be achieved at the expense of other interests (e.g., privacy protection). Thus, states adopting different models have

---

[82] Wu Baiyi and Zhang Yifei, "The Logic of *State's Return* Phenomenon and the Dilemma of Global Governance," *Academic Monthly* 1 (2021): 80.

[83] Ibid., 89.

different preferences in choosing values, which leads to the dilemma of value identification.

The history of the U.S. and the EU in exploring cooperation on cross-border data flows exemplifies the challenges of value recognition between different regulatory models. The U.S. and the EU are each other's key trade and investment partners, with frequent data flows between them.[84] However, given the significant differences between the U.S.'s economic efficiency-driven proposition and the EU's human rights protection-oriented proposition, cooperation on data transfers between the two sides has been slow to materialize. Faced with the realities of the need for economic cooperation, the U.S. and Europe reached the *Safe Harbor Agreement* in November 2000, which was upgraded in February 2016 to the *EU-U.S. Privacy Shield Framework*.[85] The two agreements, in essence, represent a compromise between the two sides on the issue of cross-border data flow. However, the Court of Justice of the European Union (CJEU) invalidated the *Safe Harbor Agreement* and the *Privacy Shield Framework* in successive judgments in 2015 and 2019.[86] Given the strong emphasis on human rights protection in the CJEU's decisions in recent years and the considerable criticism of the *Privacy Shield Framework* within the EU, some scholars believe that the CJEU's decision to invalidate the *Privacy Shield Framework* is not surprising.[87]

The successive failures of the *Safe Harbor Agreement* and the *Privacy Shield Framework* reflect profound differences in the understanding of data sovereignty between the U.S. and the EU. The EU's digital trade rules, incorporated into its international trade agreements, are based on the GDPR. With the GDPR, the EU has extended the extraterritorial application of data governance rules within its borders, further expanding its data governance jurisdiction. While the EU's GDPR has had a significant impact on the global digital trade market with its extraterritorial application and severe penalty regime, it is premature, if not impossible, to say that the global model of data governance is moving toward synchronization with the GDPR's privacy protection as the standard.[88] One of the main reasons for this is that other countries lack a historical background similar to that of the EU and a cultural acceptance of privacy protection as a fundamental human right,[89] which is also one of the reasons for the recurring failures of U.S.-EU cooperation on cross-border data

---

[84] For analysis on the trade and investment dependencies between the U.S. and EU, see CRS Report R43387, Transatlantic Trade and Investment Partnership (T-TIP) Negotiations, by Shayerah Ilias Akhtar, Vivian C. Jones, and Renée Johnson. See also, CRS In Focus IF10120, Transatlantic Trade and Investment Partnership (T-TIP), by Shayerah Ilias Akhtar and Vivian C. Jones.

[85] For the histories of negotiations between EU and the U.S. on cross-border data flow, see Xu Duoqi, "International Pattern of Personal Data Cross-border Flow Regulation and China's Response," *Legal Forum* 3 (2018): 130-137.

[86] Judgment in Case C-362/14, Maximillian Schrems v Data Protection Commissioner. Case C-311/18, Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems, EU: C: 2020: 559, Judgment of the Court (Grand Chamber) (E. C. J. July 16, 2020).

[87] Christopher Kuner, "The Schrems II judgment of the Court of Justice and the future of data transfer regulation," accessed May 9, 2025, https://www.europeanlawblog.eu/pub/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/release/1.

[88] Christopher Kuner, "Reality and Illusion in EU Data Transfer Regulation Post Schrems," *German Law Journal* 18, no. 4 (2017): 881.

[89] James Q. Whitman, "The Two Western Cultures of Privacy: Dignity versus Liberty," *The Yale Law Journal* 113 (2004): 1160, 1161 and 1169.

flows.

However, the U.S. and the EU still haven't stopped looking for a path to cooperation, driven by the practical needs. On July 10, 2023, the European Commission adopted an implementing decision on the *EU-U.S. Data Privacy Framework*. As a result, personal data from the EU can be transferred to the U.S. without further authorization from the EU. Promoted by the vast economic value of cross-border data flows, countries will continue seeking more digital economic and trade cooperation in the future; therefore, the game of constructing data sovereignty in international trade agreements will persist. Although the progress of the game among countries has been slow due to differences in political demands, economic interests, history, and culture, some countries have already demonstrated better adaptability to different models of constructing data sovereignty boundaries in international trade agreements. An example of this is Japan. Japan is a member of TPP, a contracting party to the EJEPA, and a member of the RCEP, in which Japan has accepted the data sovereignty contraction model oriented toward economic efficiency, the data sovereignty contraction model oriented toward human rights protection, and the data sovereignty expansion model under the direction of pluralistic values, respectively, demonstrating a good adaptability to different models of data sovereignty boundary construction.

Moreover, the regulatory model adopted by a state is not static, but may change in response to its real needs. For example, in late 2023, the U.S. is changing its stance on advocating for the free flow of data across borders in WTO negotiations, in an attempt to expand its own regulatory space.[90] As mentioned earlier, the EU's regulatory proposition for cross-border flows is also changing. It can be seen that, although there are specific differences in the value recognition of states adopting different regulatory models, there is still a possibility of reaching consensus between China's pluralistic-value-oriented model and the other two models, taking into account the necessity of cooperation in cross-border data flows, the diversity of national regulatory needs, and the flexibility of regulatory models.

C. Key points for constructing data sovereignty rules

The first is to strike a good balance between sovereignty interests and other interests. The data regulation position adopted by China in existing international trade agreements is "security first," which aligns with our security needs in the current complex geopolitical landscape. Given that China has become one of the world's fastest-growing digital economies, vigorously promoting digital trade may become the driving force behind China's economic growth in the new era. As a result, in international trade negotiations, China can effectively incorporate provisions to facilitate cross-border data flow, particularly as a basis for cooperation with countries that adopt an economic efficiency-oriented model.

One way to realize this is to rationalize the scope of digital trade barriers. Although the data sovereignty contraction model constructed by the U.S.'s international trade agreements has an apparent orientation toward economic efficiency,

---

[90] USTR, USTR Statement on WTO E-Commerce Negotiations, accessed May 9, 2025, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2023/October/ustr-statement-wto-e-commerce-negotiations.

the agreements concluded by the U.S. to date that contain digital trade provisions still focus on only some of the digital trade barriers, such as personal information protection, consumer protection, data localization requirements, and source code fulfillment requirements. These agreements still lack regulation on many potential barriers to digital trade, such as data filtering and blocking, disinformation, malware, and cybersecurity risks including distributed denial-of-service (DDoS) attacks.[91] If international trade agreements also regulate these barriers, international trade may continue growing, driven by the concept of innovative digital trade barriers.[92] Currently, the focus of international trade negotiations surrounding data sovereignty remains on traditional digital trade barriers, including data localization requirements and source code fulfillment requirements. In the future, the U.S. may seek to innovate digital trade barriers in international trade agreements to enhance economic efficiency further and contract the data sovereignty of other countries. However, this is likely to become a significant challenge in the future game of data sovereignty among states.

Digital trade barriers are less frequently addressed in the international trade agreements concluded by China; however, this phenomenon has been addressed in recent years. While still limiting data regulation to traditional e-commerce, the RCEP has addressed core issues of digital trade, such as the localization of facilities and the free flow of data across borders, which may serve as a stepping stone for further cooperation among China, the U.S., and the EU in future negotiations. China can actively utilize the function of early and pilot implementation of free trade zones and free trade ports to explore the digital trade barriers that China can accept for inclusion in regulations, and then promote them in some international trade agreements. Considering that New Zealand is a member of both TPP and DEPA and may incline to the economic efficiency-oriented model, China may, based on perfecting the "safety valve" of exception clauses and non-conformity measures, appropriately include the regulation of traditional digital trade barriers as the foundation for seeking cooperation in economic and trade negotiations, and explore the innovation of digital trade barriers in a "small-stepped" manner.

The second is to properly handle the collaboration and coordination of the rule of law at the domestic and international levels. Establishing the boundaries of data sovereignty involves both domestic and international law. If domestic data regulation legislation conflicts with or deviates from the obligations of concluded international trade agreements, the country may easily lose the initiative in the game of data sovereignty. In the domain of international investment law, since cross-border data flow may be considered as a form of international investment,[93] the actions of host states that impede cross-border data flow may, under certain circumstances, violate the obligations of international investment agreements requiring host states to provide national, fair, and equitable treatment or the prohibition of indirect expropriation.[94]

---

[91] Susan Ariel Aaronson, "The Difficult Past and Troubled Future of Digital Protectionism," 152.

[92] OECD, "Mapping Approaches to Data and Data Flows," Report for the G20 Digital Economy Task Force, Saudi Arabia 2020, 11-12.

[93] Zhang Sheng, "Cross-border Data Flow under the Framework of International Investment Law: Protection, Exception, and Challenge," *Contemporary Law Review* 5 (2019): 151-152.

[94] Zhang Qianwen, "The Compliance of International Investment Agreement of Data Localization Measures and China's Responses," *Studies in Law and Business* 2 (2020): 85-98.

For example, the GDPR was challenged immediately upon its publication, as it contains data localization and data minimization requirements that were alleged to violate the EU's obligations under international investment agreements concluded by the EU, which require fair and equitable treatment of foreign investors.[95] In the domain of international trade law, regulatory measures on cross-border data flows have been challenged as trade barriers. Failure to meet the conditions for lawful regulation may violate fundamental principles of international trade law, such as the non-discrimination principle.[96] In particular, with the rapid development of the digital economy and the growth of digital enterprises, the question of whether a state's measures to regulate the cross-border data flow are in breach of its obligations under international trade agreements is bound to gain attention. It may give rise to numerous international trade disputes. China has so far concluded more than 100 bilateral investment agreements and is a key member of the WTO. Many of the international trade agreements concluded by China include articles regarding market access, national treatment, most-favored-nation treatment, fair and equitable treatment, and other related provisions. Therefore, the synchronization of China's data legislation with the international trade agreements it has concluded is necessary for China to participate in the global game of data sovereignty.

The year 2021 may be regarded as the "first year" of data governance in China. Previously, China's regulations on cross-border data flow were scattered across various laws and regulations, including the *Cybersecurity Law*, *Electronic Commerce Law*, and *General Principles of the Civil Law*. In 2021, China's *Data Security Law*, *Personal Information Protection Law*, and *Regulations on the Security Protection of Critical Information Infrastructure* came into effect, establishing a domestic legislative and regulatory framework for managing cross-border data flows. From the perspective of coordinating domestic rule of law and foreign-related rule of law, China should pay particular attention, in the course of subsequent improvements to data security legislation, to ensuring that domestic laws are consistent with the obligations undertaken under international trade agreements. For example, China should stipulate the legitimacy basis of regulatory rights in the international investment agreements concluded by China, with a focus on supplementing exceptions for public order, public morals, and essential security interests; timely establish a data classification and grading system, at the same time aligning it with the data localization requirements of key infrastructure; coordinate China's data regulatory legislation with the definitions of core terms such as "essential security interests," "national security," "public order" and "public interest" in international agreements;[97] and, improve data security legislation based on recent WTO rulings and relevant decisions from international investment arbitration tribunals to align domestic legislation with international trade rules.

---

[95] Vishaka Ramesh, "Data Protection Principles Around the World. Do They Violate International Investment Law?" *Völkerrechtsblog*, 2018.

[96] e. g. Andrew D. Mitchell and Jarrod Hepburn, "Don't Fence Me in: Reforming Trade and Investment Law to Better Facilitate Cross-border Data Transfer," *The Yale Journal of Law and Technology* 19 (2017): 182; Mira Burri, "The Regulation of Data Flows Through Trade Agreements," *Georgetown Journal of International Law* 48, no. 1 (2017): 407.

[97] Zhang Qianwen, "Regulation of the IIA Exception Clause for Cross-border Data Flows," 101-102.

The third is to promote Chinese solutions through the construction of the "Digital Silk Road." China has already demonstrated part of its position on digital trade in the RCEP, and should seize the opportunity that the current international rules on digital trade are still in their infancy, to actively promote China's position on digital trade from a bilateral or regional perspective and strive for the leadership of international rules on digital trade. Although states are actively launching negotiations on e-commerce on the platform of the WTO, it is foreseeable that states will find it difficult to compromise easily in the area of digital trade and reach a set of uniform international rules on a global scale in a short period, in view of the vital value of data and the multiple dilemmas faced by the WTO. The U.S. and EU are the first to formulate unified data legislation at home and then promote their policy philosophies in the regional context through international trade agreements, based on the formation of domestic digital trade rules. This can also serve as a reference for China. The conclusion of the DEPA may also herald an easier agreement on rules for digital economy and trade on a smaller scale. Meanwhile, values and cultural differences cannot be ignored in the choice of the pilot region. China can take the opportunity of the construction of the "Digital Silk Road" and integrate the construction of international rules on digital trade to the construction of digital infrastructure, prioritize the countries under the Belt and Road co-construction framework, in particular, developing countries, to form regional alliances, and try to promote China's position on data regulation through the updating of bilateral investment agreements, negotiation of regional trade agreements, and other forms of cooperation, which can be further promoted to a broader scope under a multilateral framework. For example, China and the Association of Southeast Asian Nations (ASEAN) are in the process of negotiating the *China-ASEAN Free Trade Agreement* (CAFTA) 3.0, and half of the ASEAN member countries are parties to the *Beijing Initiative on the Belt and Road International Digital Economy Cooperation* and important partner countries in China's construction of the "Digital Silk Road". China can also explore promoting the digital trade propositions in the free trade agreement with ASEAN. One possible way to address the dilemma of value identity may be the greater commitment to building a principled framework for cooperation, drawing on the practices of the DEPA, in innovating rules for digital trade.

V. Conclusion

At the advent of the "Fourth Industrial Revolution," countries are increasingly competing for data resources and attaching greater importance to data sovereignty. Due to the fluid nature of data and the necessity of cross-border flow to realize its economic benefits, regulating cross-border data flow involves establishing a state's data sovereignty. Therefore, based on the need to improve domestic legislation and establish their own data sovereignty, states are actively constructing data sovereignty through the conclusion of international trade agreements. In the negotiation of such agreements, states have demonstrated different regulatory propositions for cross-border data flow, reflecting the tension between three sets of values: collectivism and individualism, security and freedom, and tradition and innovation.

Among these propositions, the main representative ones in the world at present are the data sovereignty contraction model driven by economic efficiency, led by the U.S., the data sovereignty contraction model oriented toward human rights protection, led by the EU, and the data sovereignty expansion model under the direction of pluralistic values by China.

General Secretary Xi Jinping pointed out that China should "actively participate in international cooperation in the digital economy sphere" and "actively participate in negotiations within international organizations concerning the digital economy, carry out bilateral and multilateral cooperation on digital economy governance, and safeguard and improve the multilateral governance system for the digital economy by voicing our opinions and presenting our solutions." In 2020, China issued the *Global Initiative on Data Security*, calling on all states "to put equal emphasis on development and security, and take a balanced approach to technological progress, economic development and protection of national security and public interests." To lay a solid foundation for participating in the game of international rules governing the digital economy and trade, China should improve the construction of data sovereignty rules promptly and strive to lead the development of international rules governing the digital economy and trade. In this process, China should balance its sovereignty interests with other interests, during which a possible practice is to explore the scope of system-acceptable digital trade barriers through free trade zones; integrate the domestic and foreign-related rule of law to synchronize China's data regulation legislation with its obligations under the international trade agreements concluded; and, starting from the bilateral or regional perspective, first carry out economic and trade negotiations with the countries similar in cultural values of China, incorporate digital trade provisions in the agreements, and proactively promote China's position.

(Translated by *ZHAO Zeming*)