Protection of the Right to Data Privacy Under the Liberalization of Digital Trade

ZHANG Ming[*]

Abstract: *In the digital era, the free cross-border flow of data and the development of digital trade are complementary. Consequently, as an inherent demand for data privacy, trade liberalization is closely linked to the right to data privacy, and data privacy protection is increasingly becoming a trade issue. However, conflicting rule settings between the two create discrepancies and result in differing rule-making approaches. The concept of the right to data privacy provides guidance and evaluative functions for the development of trade liberalization, facilitating the healthy development of digital trade. It is appropriate to treat the interaction between trade liberalization and data privacy protection in a rational way and to place them within independent systems at this stage. Data localization measures are an effective way to balance digital trade liberalization with the right to data privacy. As a data privacy protection measure, data localization has legitimacy within the trade law framework. Looking ahead, to achieve a harmonious advancement of digital trade liberalization and protection of the right to data privacy, all parties should uphold the premise of the national regulatory autonomy, and respect the data localization measures adopted by countries based on their own national conditions and personal data protection considerations.*

Keywords: digital trade ♦ right to data privacy ♦ data localization measures ♦ trade linkage

As shown by the development and application of international law, the evolution of international law after the end of the Cold War has been primarily driven by two fundamental concepts: economic globalization and human rights.[1] The field of international trade law has seen significant criticism and conflict between the concept of trade liberalization led by economic globalization and the concept of human rights. Since the outbreak of the Seattle protests[2] in 1999, the criticism of the WTO based on human rights discourse has been growing, which has triggered a transnational and interdisciplinary debate in academic circles on "trade liberalization and human rights protection" for more than a decade. Precisely because of the impact of free trade on many areas, including human rights, trade linkage, or the phenomenon of "trade and human rights," free trade has become the focus of attention and a central policy conundrum in the international system.[3]

In the digital age, the issue of trade linkage has given rise to a number of new phenomena. The free flow of data across borders that digital trade relies on has the potential to harm the privacy and security of personal data/information.[4] As a new manifestation of

[*] ZHANG Ming (张明), Postdoctoral Researcher at Nanjing University Law School, Lecturer at China Jiliang University Law School, Master's Supervisor, Doctor of laws. This paper is the phased outcome of the project "Research on China's Rule of Law Path for Maintaining the Security and Stability of Global Supply Chain" (Approval No. 2024M751358) that received funding from the 75th general grant of the China Postdoctoral Science Foundation.

[1] Robert Howse and Ruti G. Teitel, "Beyond the Divide: The International Covenant on Economic, Social and Political Rights and the World Trade Organization," in *The World Trade Organization and Human Rights: Interdisciplinary Perspectives*, Sarah Joseph et al. eds. (Cheltenham and Northampton MA: Edward Elgar Publishing, 2009), 39.

[2] The Seattle protests lasted from November 30 to December 3, 1999, when the Third WTO Ministerial Conference was held in Seattle, the United States. Around the time of the meeting, mass demonstrations erupted in Seattle. Tens of thousands of anti-globalization activists hoped to draw the WTO's attention to the trade environment, labor standards, and so on.

[3] Frank J. Garcia, "Trade and Justice: Linking the Trade Linkage Debates," *University of Pennsylvania Journal of International Economic Law*, vol. 19, no. 2 (1998): 393; John H. Jackson, "Afterword: The Linkage Problem — Comments on Five Problem," *The American Journal of International Law*, vol. 96, no. 118 (2002): 118. As for the concept of "trade linkage," there is no accurate definition in the academic circles. What scholars often refer to as "trade linkage" is the certain institutional linkage created between trade liberalization and aspects of social life such as human rights protection, so that the two can progress simultaneously. See Li Chunlin, *Research on the Relationship between Trade Liberalization and Human Rights Protection* (Beijing: Law Press • China, 2016), 51-52.

[4] Although data and information are different in meaning and connotation, there is no need to make a strict distinction between the two in terms of use of legal concepts. See Mei Xiaying, "The Legal Significance of the Distinction between

trade liberalization, the free flow of data across borders meets and conflicts with the right to data privacy, a fundamental human right in the digital age. As a consequence, the legal and policy circles have begun to pay attention to this issue. At the legal level, legislation for the protection of data privacy or personal information is being enacted around the world.[5] China's *Cybersecurity Law*, *Personal Information Protection Law* (PIPL) and supporting regulatory documents, as well as the European Union's *General Data Protection Regulation* (GDPR), are all legal responses to the protection of data privacy. At the policy level, data privacy protection is included in a growing body of policy documents. In 2021, the State Council issued the *Development Plan for Digital Economy during the 14th Five-Year Plan Period*, which emphasizes that international rules and experience should be drawn upon to explore the formulation of governance rules on major issues such as data privacy protection. The *Opinions of the Central Committee of the Communist Party of China and the State Council on Building a Data Foundation System to Better Play the Role of Data Elements* (hereinafter referred to as the "20 Articles on Data") states the need to "improve the system of compliance and regulatory rules for the whole process of data ... ensuring that the source of data in circulation is legitimate, privacy protection is in place, and circulation and transaction are standardized." Moreover, local plans for pilot free trade zones also include data privacy protection in the policy agenda.[6] It can be seen that data privacy protection has become a real issue and is receiving increasing attention.

The development of practice strikes a chord in the academic circles. In response to data privacy protection, a hot topic in the digital trade era, many scholars have entered into insightful discussions.[7] However, the issue of data privacy protection is hot due to the free flow of data across borders, which has been infinitely magnified in the era of digital trade. Therefore, it is necessary to think about the following questions: what is the linkage between trade liberalization and the right to data privacy? As digital trade liberalization gains traction, how can the right to data privacy be effectively protected? What are the boundaries of data localization measures as a data privacy protection measure? In view of these, this paper attempts to discuss the interaction between digital trade liberalization and the right to data privacy and explore a reasonable path for data privacy protection in the context of trade liberalization. It then uses China's PIPL to demonstrate that data localization is an effective measure to balance trade liberalization and data privacy protection, and puts forward suggestions for optimization.

I. The Linkage and Conflict between Digital Trade Liberalization and the Right to Data Privacy

Information and Data Concepts," *Journal of Comparative Law* 6 (2020): 151. Based on this, this article does not make a clear distinction between data and information concepts.

[5] More than 140 countries or regions have enacted laws pertaining to the protection of personal information. See Liu Junchen, "Explanation on the Personal Information Protection Law of the People's Republic of China (Draft)," npc.gov.cn (National People's Congress), http://www.npc.gov.cn/npc/c30834/202108/fbc9ba044c2449c9bc6b6317b94694be.shtml, August 20, 2021. The European Union's General Data Protection Regulation (GDPR), implemented in 2018, is the most influential among those issued by major digital economies, with the exception of China. The U.S. personal information protection legislation is mainly enacted at the state level, but it has also begun to be promoted at the federal level recently. On June 3, 2022, the United States Senate and House of Representatives jointly unveiled the draft text of the *American Data Privacy and Protection Act*. In addition, Japan's *Act on the Protection of Personal Information* (APPI), promulgated in 2003, is one of the earliest personal information protection laws in Asia, and was amended in 2015 and 2020. In January 2020, South Korea passed amendments to the *Personal Information Protection Act*, the *Credit Information Act*, and the *Act on Promotion of Information and Communications Network Utilization and Information Protection*, laying the foundation for the protection of personal information and the development of the data industry.

[6] For example, the overall plan for China (Beijing) Pilot Free Trade Zone stipulates that it will explore to set rules for key areas such as information technology security, data privacy protection, and cross-border data flow.

[7] For relevant representative literature, please refer to: Li Shuhui, "The Legislative Response to Privacy Protection in the Digital Age," *Law Science* 3 (2024): 17-31; Peng Yue, "Data Privacy Regulatory Model and Its Trade Law Expression," *Studies in Law and Business* 5 (2022): 102-117; Dai Long, "On the Protection of Personal Privacy in the Context of Digital Trade," *Contemporary Law Review* 1 (2020): 148-160; Svetlana Yakovleva and Kristina Irion, "Pitching Trade Against Privacy: Reconciling EU Governance of Personal Data Flows with External Trade," *International Data Privacy Law*, vol. 10, no. 3 (2020): 201-221; Paul M. Schwartz and Karl-Nikolaus Peifer, "Transatlantic Data Privacy Law," *Georgetown Law Journal*, vol. 106, no. 1 (2017): 115-179.

The free flow of data across borders and the development of digital trade complement each other. However, while the free flow of data across borders has spurred digital trade, it has also generated practical concerns.[8] As far as data privacy protection is concerned, the dilution of physical national boundaries makes state supervision increasingly difficult, and the protection of personal privacy faces obstacles.[9] As a result, data privacy protection has become a core focus of concern for all countries. Countries (or coalitions of countries) embrace different regulatory paths in light of the current development of their own digital trade and infrastructure as well as their legislative traditions. Data localization measures reflect the divergence of regulatory paths among various parties and are also a realistic portrayal of the linkage between the free flow of data across borders (trade liberalization) and data privacy protection (human rights).

A. The linkage between digital trade liberalization and the right to data privacy

Although trade liberalization has become an irreversible trend and has brought tangible benefits to the global community, practice has shown that trade liberalization is a two-edged sword. The negative impact of trade liberalization on basic human rights has drawn increasing attention to the conflict between trade liberalization and basic human rights. Such conflicts still persist in the age of digital trade.

First of all, the right to data privacy is a realistic embodiment of human rights in the digital age. Data rights, including the protection of the right to data privacy, are the foundation of a democratic society as well as a prerequisite for the healthy development of a digital society.[10] In the digital age, the forms of human rights are being transformed and reshaped[11] by digitalization as never before. To meet the objective development requirements in the digital age, it is necessary and imperative to adopt a new outlook on human rights and promote the transition of the outlook on human rights from the physical world to the digital world. The right to data privacy is undoubtedly the core focus of attention. In this context, the emergence of digital human rights,[12] including the right to data privacy, is a realistic response to the fundamental rights of individuals in the digital environment, and has increasingly become the stance of countries in digital trade negotiations. As the European Commission stressed, "Data protection is not red tape or a tariff. It is a fundamental right and as such it is not negotiable."[13] It can be seen that the right to data privacy receives attention in more and more countries as a core component of digital human rights in the digital age.

Second, a typical manifestation of trade liberalization in the field of digital trade is the vigorous encouragement and tireless pursuit of the unrestricted flow of data across borders. The free flow of data across borders is a spontaneous process and an inevitable result of digital trade. Therefore, pursuing the free flow of data across borders is to some degree the pursuit of digital trade liberalization. In the United States, for example, since data flow is fundamental for the digital industry, promoting the non-mandatory localization of data storage and the free flow of data across borders has become the focal point of the efforts and

[8] Ma Qijia and Li Xiaonan, "On the Construction of Regulatory Rules for Cross-border Data Flow in China," *Research on Rule of Law* 1 (2021): 93.

[9] Zhao Jun, "The Development Landscape and Rule of Law Path for Digital Economy under the Belt and Road Initiative," *China Law Review* 2 (2021): 47.

[10] Zhou Weidong, "The Constitutional Systematization of Personal Data Rights," *Law Science* 1 (2023): 32.

[11] Ma Changshan, *Law Towards a Digital Society* (Beijing: Law Press • China, 2021), 128.

[12] Although the debate over the connotation and independence of "digital human rights" is still ongoing, the human rights attribute of the right to data privacy has been increasingly recognized. For relevant literature, see Zhang Wenxian, "Human Rights Jurisprudence in the New Era," *Human Rights* 3 (2019): 21. In the paper, the author distills the concept of "digital human rights" insightfully, and believes that a manifestation of "digital human rights" is "respect and protection for citizens' (users') privacy in digital lives." In addition, for relevant literature, see Ma Changshan, "The Fourth-generation Human Rights in the Context of Smart Society and Their Protection," *China Legal Science* 5 (2019): 17; Gong Xianghe, "People's "Digital Attributes" and Their Legal Guarantee," *ECUPL Journal* 3 (2021): 77-78; Gao Yifei, "The Systematic Development of the Normative Construction of Digital Human Rights," *Chinese Journal of Law* 2 (2023): 37-51; Wang Ruxia, "On the International Pattern of Digital Human Rights Discourse and China's Choice of Path," *Legal Forum* 1 (2024): 93-102.

[13] Speech – "Towards a More Dynamic Transatlantic Area of Growth and Investment, European Commission website (October 29, 2013), https:/ec.europa.eu/commission/presscorner/detail/en/SPEECH_13_867.

negotiations of the U.S. in the field of digital trade.[14] This undoubtedly indicates a propensity for significant trade liberalization.

Finally, there is a strong link between the right to data privacy, which is part of digital human rights, and digital trade liberalization. From the perspective of international trade law, data privacy protection can be translated into trade issues in a number of ways. First, the right to data privacy has become a core concern for nations in the formulation and implementation of digital trade policies. The significance of this concern is underscored by the accelerated development of digital trade and the frequent occurrence of data privacy breaches. Consequently, countries or regions may formulate different data privacy protection standards and protection paths based on their respective policy stance and core concerns. This may lead to new digital trade barriers and hinder the development of international trade liberalization. Second, the right to data privacy will unavoidably be threatened as digital trade liberalization advances. The development of digital technology and the ease of data flow have removed the physical boundaries of the physical world, weakening individual control over data. At the same time, the social configuration of public and private spaces has changed due to the development and application of data technology, making it impossible to distinguish between the public and private domains.[15] As a result, data privacy is facing potential threats, and there is also a growing call for data privacy protection. It can be seen that digital trade liberalization and digital human rights, which are part of the right to data privacy, are closely interdependent, influencing each other.

It is noteworthy that the development of digital trade is cross-border in nature. Digital trade marks a new stage in the development of international trade and is widely practiced around the world. This also means that no country or individual involved in digital trade is immune from the conflict between digital trade liberalization and the right to data privacy. Undoubtedly, a realistic manifestation of this trend is that data privacy protection has become an increasingly hot topic in the negotiations on digital trade rules.

B. Analysis of the conflict between digital trade liberalization and the right to data privacy as well as its causes

Both the international human rights law system led by the *International Bill of Human Rights*[16] and the international trade law system centered on the WTO are important components of existing international law. Theoretically, trade and human rights should be put on an equal footing and given equal importance. However, when digital trade liberalization is in conflict with data privacy protection, the right to data privacy is not universally, fully and effectively protected. There is a distinct conflict between digital trade liberalization and the right to data privacy.

The conflict between digital trade liberalization and the right to data privacy is manifested in the contradiction between international trade rules and data privacy protection rules. Under the international trade law system, international trade rules represented by the WTO constantly promote trade liberalization, including the pursuit of the free flow of data across borders. According to the consolidated text of WTO e-commerce negotiations, despite differences and divergence in the scope and extent of obligations, most negotiating parties have put forward proposals to ensure the free flow of data across borders and are inclined toward prohibiting data localization measures.[17] Many recently concluded regional trade

[14] Chen Huanqi and Zhou Nianli, "The Core Demands of the United States' Digital Trade Rules from the Perspective of USMCA and Its Differences with China," *International Economics and Trade Research* 6 (2019): 109.

[15] Zheng Ge, "Between Encouraging Innovation and Protecting Human Rights: How the Law Rises to the Challenge of Big Data Technological Innovation," *Exploration and Free Views* 7 (2016): 81.

[16] In general, the *Universal Declaration of Human Rights* (1948) is seen as the foundation of the international human rights law system. In the United Nations system, the *Universal Declaration of Human Rights*, the *International Covenant on Civil and Political Rights* and the *International Covenant on Economic, Social and Cultural Rights* together constitute the *International Bill of Human Rights*. See *The Foundation of International Human Rights Law*, United Nations website, https://www.un.org/en/about-us/udhr/foundation-of-international-human-rights-law.

[17] WTO, WTO Electronic Commence Negotiations Consolidated Negotiating Text — December 2020, INF/ECOM/62/Rev. 1, December 14, 2020, para. B.2. (1)-para. B.2. (2).

agreements have also taken a stand on restricting data localization measures and stressed the importance of the free flow of data across borders.[18] Under the international human rights law system, the right to privacy is regarded as a basic human right, and nations are guided to better protect the right to data privacy through the formulation of international rules. Privacy and data protection have become a priority for many international organizations.[19] The *Universal Declaration of Human Rights* and the *International Covenant on Civil and Political Rights* enshrine the right to privacy as a basic human right. In the digital age, the right to privacy, as a traditional human right, is gradually introduced into the digital space, and states are required to attach importance to the protection of the right to data privacy. On December 18, 2013, the 68th session of the United Nations General Assembly adopted "resolution 68/167 on the right to privacy in the digital age," reiterating the right to privacy as enshrined in Article 12 of the *Universal Declaration of Human Rights* and Article 17 of the *International Covenant on Civil and Political Rights*, and calling upon all states to respect and protect the right to privacy in digital communication and to ensure the full and effective implementation of their obligations under international human rights law.[20] "Resolution 69/166 on the right to privacy in the digital age," adopted at the 69th session of the United Nations General Assembly on December 18, 2014, encourages the Human Rights Council to identify and clarify principles, standards and best practices regarding the promotion and protection of the right to privacy.[21] While the United Nations General Assembly resolutions are not mandatory and binding, they provide the basis for the development of international law and the rapid progress of customary rules, and may have corresponding force of law as an authoritative interpretation.[22] It is evident that in the overall international law system, the rules of international trade law and the rules of international human rights law are in conflict in terms of obligations.

The conflict between digital trade liberalization and the right to data privacy occurs for two reasons. One is that there is divergence between the two in the pursuit of values. The value of trade efficiency pursued by digital trade liberalization emphasizes the free flow of data across borders and regards measures that impede the free flow of data across borders as trade barriers. Thus, nations are required to minimize regulatory measures and trade restrictions in digital trade. In contrast, international human rights law regards the right to privacy as a fundamental human right and stresses the protection and importance of the right to data privacy. Conflict arises accordingly. The second reason is that the fragmented development of international law has exacerbated the conflict between digital trade liberalization and the right to data privacy. The fragmented development of international law will result in a tendency toward "departmentalism" and "regionalism" in international law, which in turn causes conflicts between substantive law rules.[23] As the United Nations International Law Commission states in its report *Fragmentation of International Law*, such conflict is manifested in a situation where "two or more rules and principles are both valid and applicable in respect of a situation."[24] This means that these conflicts will cause

[18] Even in the RCEP, its e-commerce chapter stipulates in principle that Parties shall not prevent the cross-border transfer of information by electronic means. See RCEP Article 12.15 "Cross-border Transfer of Information by Electronic Means."

[19] Rebekah Dowd, *The Birth of Digital Human Rights: Digitized Data Governance as a Human Rights Issue in the EU* (New York: Palgrave Macmillan, 2022), 40.

[20] UN General Assembly, *Resolution adopted by the General Assembly on 18 December* 2013-68/167. *The Right to Privacy in the Digital Age*, United Nations website (January 21, 2014), https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/449/47/pdf/N1344947.pdf?OpenElement.

[21] UN General Assembly, *Resolution adopted by the General Assembly on 18 December* 2014-69/166. *The Right to Privacy in the Digital Age*, United Nations website (February 10, 2015), https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/707/03/pdf/N1470703. pdf?OpenElement.

[22] Ian Brownlie, *Principles of Public International Law*, translated by Zeng Lingliang et al. (Beijing: Law Press • China, 2003), 11-12.

[23] Gu Zuxue, *Existence and Development of International Law as Law* (Xiamen: Xiamen University Press, 2018), 177.

[24] UN International Law Commission, Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law, United Nations website (April 13, 2006), https://documents-dds-ny.un.org/doc/UNDOC/LTD/G06/610/77/pdf/G0661077. pdf?OpenElement.

difficulties in the application of the international law rules and states are required to comply with mutually exclusive obligations.[25] In the case of data localization measures, on the one hand, under the international trade law system, data localization measures, as a domestic regulatory means with a restrictive impact on digital trade, may face negative evaluation under international trade law and it is necessary to "restrict" its existence. On the other hand, from the perspective of international human rights law, the adoption of data localization measures by a state for the purpose of data privacy protection is a practical measure to protect the right to privacy as enshrined in the *International Bill of Human Rights* and is beyond reproach. Moreover, data localization measures are considered to be a human rights protection means and are "supported." This incongruity, discontinuity and fragmentation among international sectoral law systems will inevitably lead to conflicts between digital trade liberalization and the right to data privacy, which will hinder the development of digital trade. Faced with conflicting rules of international law, states may find themselves in a dilemma where they don't know what to do or how to make choices. In this dilemma, states may be hesitant to provide adequate and necessary protection for the right to data privacy for fear of violating trade law obligations. Therefore, the fragmented development of international law not only impedes the development of digital trade, but also makes it difficult to protect the right to data privacy.

C. Realistic manifestation of digital trade linkage and conflicts: the totally different path choices of the U.S. and Europe

A review of the history of international trade shows that the United States and the European Union, both of which enjoy advanced capitalism, have far more consensus than differences in the process of trade globalization. Guided by trade liberalism, the U.S. and Europe both emphasize and promote trade liberalization. However, in the field of digital trade, despite the fact that the U.S. and the EU both emphasize the importance of the free flow of data across borders, they disagree on the importance and priority of data privacy protection and accordingly choose totally different regulatory paths.[26] The existing academic research puts it down to the difference between the paths of "market discourse" and "rights discourse."[27]

The U.S. upholds the idea of unrestricted cross-border data flow and is committed to promoting and ensuring the unrestricted flow of data across borders to fully tap the economic benefits of data flow. In terms of the conclusion of free trade agreements, the first free trade agreement signed by the U.S. that includes the issue of cross-border data flow, i.e. the *U.S.-Korea Free Trade Agreement*, emphasizes the importance of free cross-border data flow without mentioning data privacy protection.[28] In the WTO plurilateral e-commerce negotiations, the U.S., while acknowledging the importance of data privacy, stressed that "privacy issues should be addressed by privacy protection mechanisms in a manner that is least trade restrictive."[29] Objectively, the U.S. government's statement is not inappropriate, but its implicit concern that the current global data privacy protection mechanism may impose undue restrictions on trade highlights the consistent stance of the U.S. in emphasizing the

[25] Gu Zuxue, "The Diversification, Fragmentation and Orderliness of Modern International Law," *Chinese Journal of Law* 1 (2007): 139.

[26] Liu Jinhe, "China's Data Localization," *Chinese Journal of Communication*, vol. 13, no. 1 (2020): 84.

[27] For the distinction between "market discourse" and "rights discourse," see Xie Zhengshan, "Data Privacy Protection in the Data-Driven Era: From Individual Control to Fiduciary Duties of Data Controllers," *Studies in Law and Business* 2 (2020): 74-77; See Peng Yue, "The Conflict of Data Privacy Protection from the Perspective of Trade Regulation and Its Resolution," *Journal of Comparative Law* 4 (2018): 179; See Paul M. Schwartz and Karl-Nikolaus Peifer, "Transatlantic Data Privacy Law," *Georgetown Law Journal*, vol. 106, no. 1 (2017): 121-137.

[28] See *U.S.-Korea Free Trade Agreement* (KORUS) Article 15. 8 "…the Parties shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders." Certainly, the issue of "online consumer protection" is also mentioned in other provisions of the *U.S.-Korea Free Trade Agreement* (KORUS) (Article 15.5). It seems to have implications for data privacy protection, but from the text of the article, it is mainly targeted at fraudulent and deceptive marketing.

[29] WTO, Work Programme on Electronic commerce — The Economic Benefits of Cross-border Data Flows: Communication from the United States, S/C/W/382, June 17, 2019, para. 35.

priority of digital cross-border flow. Certainly, recent practice also shows that the U.S. has begun to attach importance to the protection of personal information and data privacy. On June 3, 2022, the U.S. House of Representatives and Senate released a comprehensive discussion draft on national data privacy and data security frameworks – *American Data Privacy and Protection Act*.[30] However, the draft legislation does not address the issue of cross-border data flows, but only focuses on data privacy protection. Therefore, it cannot directly prove a shift in the ranking of the cross-border data flow and data privacy protection issues in the U.S. In summary, while the U.S. does not deny due attention to data privacy protection, it is more inclined to consider the "market" and "economic interests" and emphasize the liberalization of digital trade.

Unlike the U.S., which puts too much emphasis on openness and freedom, the EU gives full attention to the protection of data privacy when promoting the free flow of data across borders. Based on its stance that human rights protection is a priority, the EU is cautious in governing the cross-border flow of data under trade rules.[31] First of all, human rights are treated as a "silver thread" that runs through all facets of the EU's trade relations with foreign countries.[32] In the field of digital trade, the EU promotes free cross-border flow of data on the basis of strong protection of data privacy. Furthermore, some of the EU's regulatory measures based on data privacy protection may conflict with high-level free trade agreements. For example, the GDPR, which has been enacted and implemented in the EU, is questioned as having a trade restriction stance such as data localization measures due to the many measures it contains.[33] Second, data privacy protection has been a core issue in the recent EU free trade agreements. In the WTO e-commerce negotiations, the EU stressed the commitment to ensuring the free cross-border flow of data to facilitate trade in the digital economy, while at the same time protecting data and consumer privacy.[34] Finally, the EU's legislation and enforcement practices in the field of data privacy protection have a strong "Brussels effect"[35] on a global scale. The EU's stringent law enforcement and the GDPR's high standards for "adequacy" have strongly promoted data privacy protection in cross-border data flows in countries. For example, South Korea's relevant laws and data privacy protection regulatory approach are deeply influenced by the EU.[36] In summary, the EU has formed a regulatory path that emphasizes data privacy protection based on the historical concept of basic human rights.

By comparing the distinct paths between the U.S. and the EU, it is easy to see that the U.S. path that emphasizes freedom and the European path that upholds data privacy protection are actually at opposite ends of the scale. While there is adequate room for the two to achieve harmony, compatibility and balance, practice has repeatedly shown that this is by

[30] See House and Senate Leaders Release Bipartisan Discussion Draft of Comprehensive Data Privacy Bill, House Committee on Energy & Commerce (June 3, 2022), https://energycommerce.house.gov/newsroom/press-releases/house-and-senate-leaders-release-bipartisan-discussion-draft-of.

[31] Xu Duoqi, "The Construction of Trade Rule System for Governing Cross-border Data Flow," *Administrative Law Review* 4 (2022): 54.

[32] Jiang Xiaohong, "The Linkage between Trade and Human Rights: On the Human Rights Objectives in the EU's Foreign Trade Policy," *China Journal of European Studies* 5 (2016): 82.

[33] Yang Fan, "The Evolution of EU Legal Supervision on Cross-border Data Flow in the Post-Schrems II Case and China's Response," *Global Law Review* 1 (2022): 182-184; See Tian Xiaoping, "The EU *General Data Protection Regulation* from the Perspective of Trade Barriers," *Journal of Political Science and Law* 4 (2019): 124; See Anupam Chander, "Is Data Localization a Solution for Schrems II?" *Journal of International Economic Law*, vol. 23, no. 3 (2020): 777; See Han-wei Liu and Shin-yi Peng, "The Legality of Data Residency Requirements: How can the Trans-Pacific Partnership Help?," *Journal of World Trade*, vol. 51, no. 2 (2017): 191-192.

[34] See WTO, Joint statement on Electronic Commerce — Eu Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce: Communication from the European Union, INF/ECOM/22, April 26, 2019, para. 2.7-2.8.

[35] The so-called Brussels effect refers to the EU's ability to unilaterally regulate global markets based on and by virtue of its market prowess. See Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford: Oxford University Press, 2020), 1.

[36] See *Joint Statement by Didier Reynders, commissioner, and Yoon Jong In, chairperson of the Personal Information Protection Commission of the Republic of Korea*, European Commission website (March 30, 2021) https://ec.europa.eu/commission/presscorner/detail/en/statement_21_1506.

no means easy. The U.S. and the EU established the "Safe Harbor Framework" and the "Privacy Shield Framework," but both were ruled to be invalid by the Court of Justice of the EU.[37] On March 25, 2022, the European Commission and the U.S. announced that they had reached an agreement in principle on a new transatlantic data privacy framework to address concerns raised by the Court of Justice of the EU in previous cases.[38] However, it remains to be seen whether the new agreement can pass the review by the European Data Protection Board and finally be translated into legal documents pursuant to the requirements of the GDPR.

In conclusion, there is a close linkage and practical conflict between digital trade liberalization and the right to data privacy. This connection and conflict are realistically manifested by the distinct policy and regulatory paths represented by the U.S. and European paths. The nub of the matter is: how can the right to data privacy be effectively protected at a time when increasing attention is paid to the benefits of trade liberalization? The root of this problem lies in the relationship between digital trade liberalization and the right to data privacy as well as the choice of paths.

II. The Relationship between Digital Trade Liberalization and the Right to Data Privacy as well as the Choice of Paths

The choice of value for trade liberalization and data privacy protection is one of the root causes of the growing differences in the regulatory practices in the free cross-border flow of data in countries. This indirectly affects the policy stance of countries, which in turn influences the protection of the right to data privacy. The discussion on the relationship between digital trade liberalization and the right to data privacy is the theoretical starting point for exploring a balance between data privacy protection and trade liberalization in the era of digital trade. It is also a natural requirement for perfecting the protection of the right to data privacy.

A. The rational positioning of the right to data privacy in the process of digital trade liberalization

The issue of the status of human rights in trade law is an issue to be urgently addressed in the discussion of the relationship between international human rights law and the WTO legal system.[39] In the era of globalization, "data and information may promote and develop human rights, but may also threaten and infringe human rights."[40] The cross-border flow of data prompted by digital technology and digital trade has undoubtedly made it more difficult to protect data privacy. The protection measures for the right to data privacy, such as data localization measures, may hinder trade liberalization, but the right to data privacy also plays a positive role in facilitating digital trade to a certain extent.

From the perspective of international trade rule-making, the right to data privacy is somewhat in a position guiding the formulation and development of digital trade rules. For a long time, human rights have provided an independent value guidance in the development of international trade to prevent excessive pursuit of economic and efficiency value in international trade. In addition to value guidance, human rights play a role as an institutional

[37] On the judgment on the "Safe Harbor Framework," see Judgment of the Court, Maximillian Schrems vs. Data Protection Commissioner (Case C-362/14), Court of Justice of the European Union website (October 6, 2015), https: /curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=; Regarding judgment on the Privacy Shield Framework, see press release No. 91/20, The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield (Case C-311/18), Court of Justice of the European Union website (July 16, 2020), https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf.

[38] See European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework, European Commission website (March 25, 2022), https://ec.europa.eu/commission/presscorner/detail/en/ip_22_208 7.

[39] Thomas Cottier, Joost Pauwelyn and Elisabeth Bürgi Bonanomi, "Linking Trade Regulation and Human Rights in International Law: An Overview," in *Human Rights and International Trade*, Thomas Cottier, Joost Pauwelyn and Elisabeth Bürgi eds. (Oxford: Oxford University Press, 2005), 3.

[40] Ma Changshan, "The Fourth-generation Human Rights in the Context of Smart Society and Their Protection," *China Legal Science* 5 (2019): 10.

guidance. Human rights provide a normative framework for substantively adjusting trade policies and the trade regime and offer guidance and assistance to trade policymakers in redesigning the international trade regime.[41] The rights value upheld by the right to data privacy stipulates the minimum objectives and requirements of data privacy protection, and emphasizes that data privacy protection should be ensured as a basic obligation. The exception clauses in the cross-border data flow clause and the data localization clause in free trade agreements reflect the institutional guidance and bottom line for the right to data privacy to a certain extent. During the *United States-Mexico-Canada Agreement* (USMCA) negotiations, the U.S. proposed the removal of exception clauses to facilitate data flow across borders to a greater extent. In response, Canada made it clear that it was difficult to accept this proposal and stressed the importance of the exception clause for privacy protection.[42]

From the perspective of the implementation of international trade rules, the right to data privacy occupies an evaluation position in the implementation of digital trade rules. On the one hand, the right to data privacy is increasingly becoming a criterion for evaluating the legitimacy of digital trade rules. To realize the free flow of data across borders, the U.S. and the EU reached and implemented "Safe Harbor" and "Privacy Shield" agreements, which were regarded as key agreements underpinning their digital trade. However, both agreements were declared invalid by the Court of Justice of the EU, primarily because of concerns about data privacy risks. The ruling by the Court of Justice of the EU exacerbated uncertainty about the development of digital trade between the U.S. and the EU. On the other hand, in addition to legal evaluation, the right to data privacy potentially constitutes one of the moral evaluation criteria for the implementation of digital trade rules. The protection of human rights undoubtedly claims the moral high ground. For a long time, international trade rules have been heavily criticized by human rights activists, which is a realistic manifestation of moral evaluation. Therefore, whether it is conducive to the realization of basic human rights has actually become an evaluation factor for the implementation of digital trade rules.

To sum up, the right to data privacy plays an important role in digital trade liberalization. This is favorable to the healthy development of digital trade and the optimization of digital trade rules. The legal protection of data privacy also creates a reliable environment with trust and confidence for digital trade.[43] Based on this, it is necessary to further think about how to address the path of interaction between trade liberalization and the right to data privacy.

B. The dual path of interaction between digital trade liberalization and the right to data privacy

The importance of the free cross-border flow of data to international trade liberalization as well as the core value of the right to data privacy as a basic human right in the era of digital trade have received universal recognition and attention. In spite of this, the path of interaction between the two is still unstable because of the novelty of trade linkage. Effective coordination between the two has not yet been reached precisely because of a lack of stable interaction. In view of this, the analysis of the linkage between trade liberalization and human rights somewhat reflects the choice of path for the interaction between trade liberalization and human rights.

First of all, a traditional view that explains the interaction between trade and human rights is the adherence to the efficiency priority theory of classical liberal economics that "free trade can enhance global welfare." Based on this, trade liberalization is prioritized and human rights are at a disadvantage when dealing with issues of trade liberalization and human rights protection. To be frank, this view is somewhat rational in addressing the issue of linkage between traditional trade liberalization and human rights, because the linkage issue of

[41] Andrew T.F. Lang, "Rethinking Trade and Human Rights," *Tulane Journal of International and Comparative Law*, vol. 15, no. 1 (2007): 389.

[42] Chen Huanqi and Zhou Nianli, "The Core Demands of the United States' Digital Trade Rules from the Perspective of USMCA and Its Differences with China," *International Economics and Trade Research* 6 (2019): 108.

[43] Peng Yue, "The Trade Law Dimension of Cross-border Data Privacy Protection," *Journal of Law Application* 6 (2022): 28.

traditional trade is more concerned with basic human rights in the physical world, such as the right to food, the right to the environment, and the right to health. The realization of these basic rights depends on the improvement in material life and technology. By exploiting the comparative strengths of each country, free trade gives a positive incentive to the economic growth of the trading countries and even the world, thereby ensuring the protection of traditional human rights. However, this is not the case for the realization of digital human rights in the digital age. Digital trade liberalization does not necessarily bring positive benefits to digital human rights, including the right to data privacy. To some extent, it is precisely the rapidly developing digital technology and digital trade that put the right to data privacy in jeopardy and increasingly highlight its significance. In this context, it is obviously no longer a wise choice to emphasize the facilitation of human rights protection by trade liberalization based on its contribution to the welfare of society as a whole.

Second, different from those preaching the positive impact of trade liberalization on the protection of human rights, critics are more concerned with the negative effects of trade liberalization and therefore take a fundamentally critical stance on the multilateral trade regime.[44] In the eyes of critics, human rights are a value orientation that comes before trade, and trade is merely a means to realize human rights. While this view is somewhat rational, its overly radical stance is not objective and is inimical to solving the problem of trade linkage. The risks facing the right to data privacy cannot totally negate the positive effects of digital trade liberalization on fundamental rights such as the right to development. It is also not realistic to use trade as an instrument for human rights development. In modern society where the value of efficiency is highly prized, there is no success story of achieving human rights objectives through trade liberalization. In contrast, human rights are more of a tool for putting right the overemphasis on the value of efficiency. The right to data privacy also plays the role of a corrective tool.

Third, the constitutional approach incorporates constitutional thinking into international trade law and is of the view that human rights should be incorporated into the WTO agreements to achieve systematic integration of the two. The theory of rights-oriented trade advanced by scholar Petersmann based on the principles of the EU constitution and its practice has caught widespread attention.[45] Based on his view, the rights-based stance should be pursued in the study of the relationship between trade and human rights, and then the relationship between trade and human rights in international law should be established based on human rights. While this approach is a great innovation in addressing the relationship between trade and human rights and can effectively deal with the fragmentation of international law, it does not seem feasible to address trade and human rights issues based on the concept of rights as far as trade liberalization and the right to data privacy protection are concerned. At the theoretical level, there is no proper explanation for the idea of digital trade freedom as a fundamental human right. Despite the fact that digital trade liberalization and human rights protection both aim to improve the well-being of humanity as a whole, the same goals do not mean consistency in positioning. Unlike human rights, which are based on the "human" stance, digital trade freedom is founded on the position of the state. At the same time, unlike the "inherent nature" of the right to data privacy, digital trade freedom is still largely reflected in the value of instrument at the level of efficiency. From a practical standpoint, it remains to be seen whether the constitutional approach can be "feasible" in the era of digital trade. The rivalry between the U.S. and the EU has exposed the current divergence between the world's two largest trading bodies in terms of human rights and trade freedom, and there is no immediate solution. As mentioned above, compliance with the

[44] For discussion on critical theory, see Li Chunlin, "Research on the Relationship between Trade and Human Rights: Approach Criticism and Reconstruction," *Tribune of Political Science and Law* 4 (2014): 29-40.

[45] Ernst-Ulrich Petersmann, "Time for a United Nations 'Global Compact' for Integrating Human Rights into the Law of Worldwide Organizations: Lessons from European Integration," *European Journal of International Law*, vol. 13, no. 3 (2002): 629-637; See Ernst-Ulrich Petersmann, "Human Rights and the Law of the World Trade Organization," *Journal of World Trade*, vol. 37, no. 2 (2003): 268-280.

obligation with regard to digital trade freedom is shrinking the domestic policy space for the states to protect human rights. In the face of such as dilemma, it is difficult for the constitutional approach to become mainstream in the era of digital trade.

Finally, the theory of exceptions and balance occupies an important place in the current research on trade liberalization and human rights. The theory of exceptions and balance argues that some trade rules adopt a flexible approach to achieving human rights objectives, including by setting up "exception clauses" to provide a mechanism for human rights protection.[46] However, it is doubtful whether the right to data privacy can be effectively protected through exception clauses. On the one hand, since the WTO came into being in the era of traditional trade, it is doubtful whether the WTO's exception clause can be extended to the protection of the right to data privacy.[47] On the other hand, as digital trade rules are being issued one after another, the exception clauses are largely the same as those in traditional trade rules. Consequently, it is impractical to attempt to provide effective protection for data privacy through rule interpretation alone. The general exception clause is considered to be an enabling provision, i.e., granting the state the right to be immune from legal liability by invoking the general exception in the event of a breach of an agreed obligation.[48] This model of giving the states the right of defense means that the general exception clause does not mandate the states to establish an effective data privacy protection system. Therefore, it deserves careful consideration whether the exception clause can effectively realize the protection of human rights such as the right to data privacy in the process of application.

Based on this, there are still some misfits and imbalance in the existing choice of path for the interaction between trade liberalization and human rights when it comes to the protection of the right to data privacy. In the era of digital trade, it is still necessary to consider and explore the path of interaction between trade liberalization and the right to data privacy.

C. The choice of path for interaction between trade liberalization and the right to data privacy in the era of digital trade

The intension and extension of the right to data privacy have not yet been accurately defined and the digital trade rules are still in the stage of development. In this context, trade liberalization and data privacy protection can be considered being put under the framework of trade law and human rights law, respectively, thus promoting development through mutual operation and running-in. Although there are inherent and challenging drawbacks (such as the fragmentation of international law) to putting trade liberalization and the right to data privacy under different legal frameworks for limited interaction to explore their gradual integration, it is practically necessary and inherently beneficial to separate trade liberalization and the right to data privacy in the current environment.

First, trade and human rights essentially belong to two separate systems, and it is difficult to achieve institutional integration. In the era of digital trade, this difficulty still exists and is showing a tendency to be further complicated. The reason is that the fundamental focus of dispute between the right to data privacy and trade liberalization is related to the degree of the free flow of data, while the free flow of data concerns the foundation of the development of digital trade. Therefore, unlike the traditional trade linkage issue, which mainly concerns the side issues of international trade development, the conflict between the right to data privacy and trade liberalization directly concerns the fundamental core issue of digital trade development. This makes the coordination between the two even more difficult.

Second, countries differ in the demands for data privacy protection rules because the levels of digital infrastructure construction and the severity of data privacy protection vary from country to country. Therefore, it is difficult to reach a consensus on trying to set unified

[46] Shi Yewei, "The Improvement of the Mechanism for Interaction between Trade Freedom and Human Rights Protection in the Context of Global Epidemic," *Law Science* 7 (2020): 96.

[47] Svetlana Yakovleva and Kristina Irion, "Pitching Trade Against privacy: Reconciling EU Governance of Personal Data Flows with External Trade," *International Data Privacy Law*, vol. 10, no. 3 (2020): 202.

[48] Ma Le, "The Value Orientation and Judicial Logic of the Application of General Exceptions to GATT," *ECUPL Journal* 1 (2015): 17-18.

and mandatory data privacy protection rules within the framework of international trade law. The technological gap in digital infrastructure between developed and developing countries has invisibly widened the differences between them, making it difficult to set unified standards that are realistic and feasible. For developed countries, they are unable to reach consensus among themselves due to differences in value positions. This makes it difficult for them to cooperate and reach agreement under the framework of international trade law. This is different from the unanimous position of developed countries on traditional trade linkage issue. As a result, it is more realistic and feasible at the current stage to explore and implement independent data protection rules with a guiding role, as is the case with recent free trade agreements.[49]

Third, there are inherent drawbacks to incorporating data privacy protection issues into trade agreements. Data privacy protection is essentially a matter of data governance, while data governance and trade governance are at different stages. Global trade governance has entered a highly developed phase, while data governance is still in its infancy. The rash act of including data governance issues in trade agreements will hinder the development of data governance. Moreover, the full inclusion of digital governance issues in trade agreements may also discourage attempts to diversify data governance.[50] Therefore, data governance requires a more systematic and diversified response solution. A simple path of trade governance obviously cannot meet the demands of the right to data privacy protection.

Finally, the history of international trade shows that placing trade liberalization and human rights under different systems for competition and joint progress is the normal interaction between the two. This state of interaction is embodied in the "mechanism transfer" under international law-making strategies.[51] In the field of trade-related intellectual property rights, for example, when the high standards of intellectual property protection harm public health and thus cause a crisis to the right to health, the United Nations public health system represented by the WHO ensures the protection of the right to health as a basic human right through the "mechanism transfer" strategy.[52] In the current context that digital trade rules cannot provide a unified solution, it is also a good practice to put trade liberalization rules and the right to data privacy rules in different systems for maintaining their interaction.

In summary, if the relationship and interaction between digital trade liberalization and the right to data privacy is viewed rationally, it is still appropriate to put the two in two independent systems. This is required for the establishment of digital trade rules, and it is also a practical requirement for the facilitation of digital trade. It is necessary to further consider how to explore and achieve "moderate" data privacy protection to ensure effective protection of the right to data privacy in trade liberalization.

III. Data Localization Measures: Protection of the Right to Data Privacy in Digital Trade Liberalization

A practical problem to be solved urgently is how to ensure the protection of the right to data privacy in the context of trade liberalization. In the current state, data localization measures can be seen as a realistic measure to balance their relationship. Further consideration must be given to the legitimacy of data localization measures under the framework of trade law as a data privacy protection (human rights) measure. In the case of China, how should the data localization measures in China's PIPL be further optimized?

[49] For example, in the RCEP, the chapter on e-commerce provides that: "In the development of its legal framework for the protection of personal information, each Party shall take into account international standards, principles, guidelines and criteria of relevant international organizations or bodies." see RCEP Article 12.8: Online Personal Information Protection "In the development of its legal framework for the protection of personal information, …"

[50] Peng Yue, "Digital Trade Governance and Its Regulatory Path," *Journal of Comparative Law* 4 (2021): 171.

[51] In the process of discussing the changes in international rules for intellectual property, some scholars initially combined the concept of "field transfer" with the theory of international regime, and put forward the concept of regime shifting. See Laurence R. Heifer, "Regime Shifting: The TRIPS Agreement and New Dynamics of International Intellectual Property Lawmaking," *Yale Journal of International Law*, vol. 29, no. 1 (2004): 1-83.

[52] Gu Zuxue, *Existence and Development of International Law as Law* (Xiamen: Xiamen University Press, 2018), 399-400.

A. Data localization measures to balance trade liberalization and data privacy protection

Data privacy protection and digital trade liberalization are inextricably linked and mutually reinforcing.[53] The balance and coordination between the two will also become a topic of digital trade of concern to all parties for a long time to come. At present, there is a growing trend to reconcile trade liberalization with the right to data privacy. Without any doubt, data localization measures play an important role in data privacy protection under the trade law system.

Judging from the trend of coordination between trade liberalization and the right to data privacy, there is a growing call for strengthening data privacy protection in the field of international human rights law. Such a trend has begun to influence the development of international trade law to draw attention to data privacy protection. As a result, international trade law has begun to pay attention to the protection of the right to data privacy and gradually strengthen the protection of data privacy. When it comes to the issue of data privacy protection, even the U.S., which pursues the free flow of data across borders, does not totally deny the importance of data privacy protection. In the *Trade in Services Agreement* (TiSA) negotiations aimed at liberalizing high-standard trade in services, developed countries such as Canada, Japan and South Korea also emphasized the importance of data privacy protection.

Data localization measures are a data privacy protection means adopted globally. Recently, to reduce the risk of data leakage to personal data privacy in cross-border data flow, countries begin to take preventive measures to restrict data flow. Data localization measure is the most common of these preventive measures. In the international trade law system, the coordination between trade liberalization and data privacy protection in data localization measures is reflected in three areas. First, the provisions pertaining to data localization measures recognize the basic orientation of data privacy protection in the trade law system. For example, in the Regional Comprehensive Economic Partnership (RCEP), each party makes it clear that each party is obliged to "seek to ensure the security and confidentiality of communications," which reflects the guiding role of the rules.[54] Second, the existing rules specify the limits of data localization measures adopted by countries to a certain extent, which reflects the evaluation role of the rules. Third, the implementation of data localization measures has played a practical role to a certain extent. Existing studies also show that "the practice of avoiding the national security hazards and personal privacy risks that may arise from cross-border data flow through data localization and retention generally has a good effect."[55]

B. Consideration of the legitimacy of data localization measures from the perspective of trade law

Data localization measure is a typical data privacy protection means. It is necessary to examine it as a data privacy protection measure from the perspective of trade law. This is also important for achieving a balance between trade liberalization and data privacy protection. From the perspective of international trade rules, the international trade rules represented by the general exceptions to *General Agreement on Trade in Services* (GATS) provide a legitimate and legal basis for data localization measures. The general exceptions to GATS specify some exceptions that specifically apply to trade in services, one of which concerns the protection of personal privacy. Therefore, the nub of the matter is whether the invocation of data localization measures can meet the basic requirements of the general exception clause.

The application of the general exceptions to GATS is subject to a strict method of judgment. In accordance with Article 14 of the GATS, the general exceptions to GATS

[53] Dai Long, "On the Protection of Personal Privacy in the Context of Digital Trade," *Contemporary Law Review* 1 (2020): 158.

[54] See RCEP Article 12.8.1 "Each Party shall adopt or maintain a legal framework which…"

[55] Xu Duoqi, "The International Pattern of Regulation of Cross-border Flow of Personal Data and China's Response," *Legal Forum* 3 (2018): 135.

consist of the preamble and specific exceptions. According to the analysis steps of the expert panel and the appellate body, a "two-step analysis" method should be adopted to ascertain whether a measure meets the general exception clause. In other words, whether the specific measure is a specific exception should be identified first before determining whether the measure is implemented in a manner that meets the requirements of the preamble to the general exception clause.[56]

In terms of the judgment of compliance of specific exceptions, because the general exception clause explicitly includes privacy protection in the articles, the adoption of data localization measures for the purpose of data privacy protection may be in principle in line with the specific circumstances of the general exceptions to GATS. However, whether data localization measures meet the requirements of the general exceptions to GATS remains to be judged. Specifically, the privacy exception is stipulated in item (c) of the general exceptions to GATS clause. The WTO dispute settlement panel further clarified the legal criteria for judging Article 14 (c) of the GATS in the "United States gambling case," namely: (1) the measure must be designed to "ensure compliance" with laws and regulations; (2) "Laws or regulations" shall not be contrary to the WTO agreements; (3) The measure is "necessary."[57] In line with this idea, first, data privacy protection is one of the primary goals of the implementation of data localization measures. Therefore, data localization measures are implemented at least to a certain extent to ensure compliance with reasonable laws and regulations. Second, regarding whether the laws and regulations on data privacy protection are contrary to the WTO, Article 14 (c) of the GATS provides a non-exhaustive list in the form of open-ended enumeration, which includes laws and regulations pertaining to privacy protection. The nub of the matter is whether the relevant laws and regulations are in conflict with WTO rules and obligations, including the non-discrimination principle. In this case, it is necessary to make a judgment based on the content of data localization measures. Finally, in terms of the necessity of relevant measures, it should be determined by considering a series of factors, including the importance of the interests or value pursued by the members, the degree of contribution of relevant measures to the realization of policy objectives, the extent to which relevant measures restrict trade, and the extent to which the members protect the public interest and values as well as less trade-restrictive alternative measures. Of these factors, key consideration should be given to the importance of the interests or value pursued, the contribution of relevant measures to the realization of policy objectives, and the extent to which relevant measures restrict trade.[58]

In terms of whether data localization measures meet the requirements of the preamble to the general exception clause, it is necessary to judge whether the implementation of data localization measures based on data privacy protection considerations constitutes a means of arbitrary or unjustifiable discrimination between countries in similar situations or constitutes a disguised restriction on trade in services. The preamble to the general exception clause does not target the specific content of the relevant disputed measure, but the manner in which the measure is implemented. This is to ensure that the general exception clause is not abused.[59] Therefore, data localization measures implemented for data privacy protection should be implemented in good faith. If the implementation of certain data localization measures may impose an unreasonable burden on foreign companies and then place them at a clear

56 See Report of the Appellate Body, United States — Standards for Reformulated and Conventional Gasoline, WT/DS2/AB/R, April 29, 1996, page 22; See Report of the Panel, United States — Measures Affecting the Cross-border Supply of Gambling and Betting Services, WT/DS285/R, November 10, 2004, para. 6. 449.

57 See Report of the Panel, United States — Measures Affecting the Cross-border Supply of Gambling and Betting Services, WT/Ds285/R, November 10, 2004, para. 6. 536.

58 See Report of the Panel, United States — Measures Affecting the Cross-border Supply of Gambling and Betting Services, WT/DS285/R, November 10, 2004, para. 6. 542.

59 See Report of the Panel, United States – Measures Affecting the Cross-border Supply of Gambling and Betting Services, WT/DS285/R, November 10, 2004, para. 6.581. See Report of the Appellate Body, United States — Measures Affecting the Cross-border Supply of Gambling and Betting Services, WT/DS285/AB/R, April 7, 2005, para. 339.

disadvantage in competition with domestic firms, such measures can hardly meet the requirements of preamble to the general exceptions.

C. Effective data privacy protection: Optimization of data localization measures in China's PIPL

The PIPL contains a series of data localization measures. It provides more specific and restrictive provisions on the cross-border provision of personal information. However, China lacks a system for the protection of the right to privacy in digital trade mechanism and privacy value is not protected.[60] In the context of trade liberalization, how the PIPL brings about a balance between trade liberalization and data privacy protection still needs careful consideration.

First, in the process of implementation, the PIPL may consider further harmonization and coordination with internationally accepted standards on data privacy protection. Internationally accepted data privacy protection rules have an increasingly deep influence on digital trade. From the perspective of the PIPL, the cross-border provision of personal information shall be subject to security assessment organized by the national cyberspace department or personal information protection certification performed by the relevant specialized institution. This makes it possible to align the PIPL with the standards of international organizations. This is also a realistic requirement for China to comply with the recently concluded RCEP agreement.[61] Alignment with the standards of influential international organizations can not only promote the effective protection of data information by data controllers, but also help them better integrate into the global data market and thus integrate into the global digital trade market.

Second, in the process of implementation, the PIPL may consider further enacting and improving the Chinese version of the standard contractual clauses. Article 38 of China's PIPL stipulates the basic conditions for the cross-border provision of personal information. Under the regulations, in addition to passing the security assessment, an information provider can also meet the requirements of cross-border provision of information by entering into a contract with an overseas information recipient. Essentially, such contracts are concluded between private entities based on standard contracts provided by government bodies (i.e., cyberspace department), and, therefore, they still show the characteristics of public power. As a result, when China creates its distinctive standard contract, the cyberspace department should exercise prudence in formulating the contract terms to avoid upsetting the balance between privacy interests and trade interests. Overly redundant standard contracts will inevitably be questioned for interfering with the autonomy of will of the contract. In this regard, because information security and privacy protection are involved, the standard contract may consider setting clear obligation clauses for information transmission path, receiving and storage as well as sub-licensing. As for the development and use of information, a standard contract should not unduly include it in the scope of mandatory terms.

Third, in the process of implementation, the PIPL should promote the internationalization of cross-border provision rules. The practice of the GDPR has amply demonstrated that the internationalization of intra-domain rules has a positive effect on the protection of data privacy and even participation in global digital trade activities. If China's personal information protection certification standards and security assessment criteria can be promoted globally, the picture for Chinese enterprises to participate in the global data market and trade market will be brighter. In this regard, China may consider promoting its rules for the cross-border provision of personal information through its Belt and Road Initiative.

Conclusion: The Joint Development of Digital Trade Liberalization and Protection of the Right to Data Privacy

[60] Li Shuhui, "The Legislative Response to Privacy Protection in the Digital Age," *Law Science* 3（2024): 25.

[61] See RCEP Article 12.8.2, "In the development of its legal framework for the protection of personal information, each Party shall take into account international standards, principles, guidelines and criteria of relevant international organizations or bodies."

Based on the above research, data localization measures – the core focus of attention in digital trade development, essentially reflect the trade linkage issue in the era of digital trade, i.e. the linkage between digital trade liberalization and right to data privacy. What deserve serious consideration are issues promoting the protection of the right to data privacy, exploring the interaction between the two and improving the quality and efficiency of their interaction. In this regard, international trade rules and data privacy protection rules should uphold the attitude of mutual respect and reverence, respect each other's interest demands, maintain their basic boundaries, and exercise prudence in intervening in each other's governance areas.

As digital trade is booming, the intervention of international trade rules in data privacy protection should be based on the premise of respecting the regulatory autonomy of each country. At present, the development of digital trade rules restricts the autonomy of countries to adopt data privacy protection measures to a certain extent. Although the response of international trade rules to digital trade is significant for trade globalization, the strong intervention of international trade rules in data issues is also a reason for the conflict between trade globalization and data privacy protection. Based on this, for the sake of healthy interaction between digital trade rules and data privacy protection rules, international trade rules should exercise prudence in intervening in data privacy protection issues on the basis of fully respecting the regulatory autonomy of each country. This gives countries more autonomy to adopt data privacy protection measures based on the rules of international human rights law and their own considerations. Certainly, the prudent intervention of international trade rules on data privacy protection issues does not necessarily indicate the necessary legitimacy of all data privacy protection measures. In fact, data privacy protection is essentially a domestic regulatory measure. Regarding domestic regulatory measures, international trade rules have their unique judgment path of "factor trade-off analysis." It is unnecessary to overemphasize the free flow of data across borders in international trade rules and to impose restrictions on data privacy protection measures. Therefore, from the perspective of international trade, international trade rules should uphold the basic stance of respecting regulatory autonomy for data privacy protection measures. With respect to the data localization measures, on the premise of not constituting unnecessary trade restrictions, international rules on digital trade should respect the data localization measures taken by countries based on their national conditions and personal data protection considerations. In the context of the large gap between the construction of digital infrastructure and the development of digital trade, promoting unified international rules for data localization on the premise of respecting domestic regulatory autonomy not only meets the interest demand for trade liberalization, but also satisfies the basic interest demand of developing countries for digital trade.

Whether it be digital trade rules or data privacy protection rules, China, as an emerging digital powerhouse, should participate in the formulation of international rules. This is not only a natural requirement for China to participate in global digital trade, but also an inevitable requirement for it to be more actively involved in global digital trade governance. In this way, China can enjoy more dividends accruing from the development of digital trade.

(Translated by *NI Weisi*)