

Paradigm Shift of European Union (EU) in Cross-border Data Flow Supervision — From the Perspective of Digital Services Legislation

Xia Han*

Abstract: From the perspective of regulatory entities, arenas for supervising digital services trade include bilateral, multilateral, and regional trade cooperation mechanisms. The EU is committed to constructing an open and secure digital trade environment, eliminating unreasonable restrictions on cross-border data flows, and promoting the enhancement of discourse power in digital trade rule-making by designing the terms of trade agreements to include digital trade issues. The EU has made numerous endeavors in the field of digital governance in recent years, and new internal legislation has sparked debate. While attaching great importance to the free cross-border flow of data, the EU maintains high standards for personal data privacy and data security. In order to promote the development of local industries, and small and medium-sized digital enterprises within the EU, and protect the personal data of EU citizens, the EU has become more stringent in its regulation of platform businesses from external markets in recent years. The robust regulatory model established by the EU digital legislation can serve as a guide for China as it develops a regulatory system for digital services to suit its own needs and standards.

Keywords: Cross-border Data Flow Regulation, EU Data Legislation, Data Sovereignty

I. INTRODUCTION

Digital services trade, which has transformed how services are traded and has become the primary form of services trade among countries, is the result of the growth of digital information technology.¹ The world economy was subjected to a severe slowdown during the global pandemic of COVID-19, but the growth

* Xia Han, Lecturer, Belt and Road College, Zhejiang International Studies University. Email: xiahancora@zisu.edu.cn.

¹ Qi Junyan and Qiang Huajun, Do Digital Services Trade Restrictions Affect Service Exports? Based on the Empirical Analysis of the Digital Service Industry, *World Economy Study*, No. 9, 2021, p. 37.

momentum of the new digital services trade remained strong. First, the pandemic had far less impact on the emerging service industries operating digitally. Additionally, the pandemic has sped up the traditional service industry's digital transformation and encouraged the growth of new digital service sectors.² The regulations applicable to digital services trade have swiftly changed as a result of the rapid expansion of digital trade, particularly in recent years. The dominance of legislation in digital trade, especially in the trade of digital services, has turned into an area of competition for major economies as the global economic landscape enters a phase of adjustment and multilateralism declines.³ In recent years, debates on topics like data sovereignty, the extraterritoriality of data regulation, and jurisdictional conflicts have been sparked by the EU's legislation on digital markets and services.⁴ Coordination and cooperation in legal regulation of digital services between nations and across regions is becoming more and more important. From the standpoint of rule-making, the EU is developing a more comprehensive legal framework for the trade of digital services, and its governance model for cross-border data flow is undergoing dynamic changes for the purpose of rule-making.⁵ The EU's digital legislation has a significant impact on international trade. On the one hand, it possesses the public law characteristic of coordinating the domestic regulations of member states; on the other hand, it is inextricably linked to the development of its legislative technology, regulatory concepts, and the scientific design of the regulatory

2 Li Zhengyang, Challenges and Countermeasures for High-quality Development of China's Service Trade in the Context of the COVID-19, *Journal of Commercial Economics*, No. 1, 2022, p. 149; Zhang Qi, et al., International Rules of Digital Trade: Trends and Construction Paths, *Globalization*, No. 1, 2022, pp. 70-71.

3 Sun Jin, et al., Current Situations, Challenges and Reshaping of China Digital Trade Regulations: Centered on Competitive Neutrality, *Social Sciences Abroad*, No. 4, 2020, p. 51; Wang Tuo, A Comparative Study of Digital Services Trade and Related Policies, *Intertrade*, No. 9, 2019, p. 80.

4 Yao Ling, EU's New Trade Policy and Its Impact on China-EU Economic and Trade Relations, *Intertrade*, No. 7, 2021, p. 63; Ye Kairu, "Long-arm Jurisdiction" in Data Flow Regulation: Originalist Study on GDPR of EU, *Law Review*, No. 1, 2020; Mira Burri, The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation, *UC Davis Law Review*, Vol. 51, 2017, p. 92.

5 Li Shigang and Bao Dingyurui, New Directions to Large Digital Platform Regulation: Specialized Regulatory Structure, *Ex Ante Rules and Dynamic Regulation System — A Study on EU Digital Market Act*, *Law Science Magazine*, No. 9, 2021, pp. 77-88; Yao Ling and Qin Lei, EU's New Trade Policy and Its Impact on China-EU Economic and Trade Relations, *Intertrade*, No. 7, 2021, pp. 61-65.

mechanisms themselves.⁶

Since the end of World War II, the EU has actively promoted bilateral and regional trade agreements as a model for economic regionalization and cooperation. Trade regulations frequently model their cross-border data flow and non-localized data storage systems in national or regional laws. The EU encourages the development of trade policies through legislation, and its current legislation imposes increasingly stringent restrictions and legally obligatory duties when it comes to the subject of cross-border transfer of personal data.⁷ The EU is dedicated to boosting the competitiveness of the digital economy as it has lagged behind China and the United States in the development of digital trade. One of the legislative goals of the EU is to stop the United States from endangering the network and regional security of the EU by making use of its advantages in the internet industry from the standpoint of data management and data sovereignty.⁸

This article focuses on the EU's legislation governing digital services. Based on the historical evolution of EU legislations, and the current challenges and practical considerations in regulating international trade and cross-border data flow, it reviews and analyzes the legislative framework and key mechanisms of the EU in the field of digital services trade. On this basis, it also analyzes and differentiates China's data security laws, optimization of digital market supervision, coordination and cooperation with other nations' digital trade

6 In terms of basic concepts, the interpretation of the concepts of "data controller" and "data processor" in the Data Protection Directive and the General Data Protection Regulations is not limited to entities situated/registered within the EU region, but equally applies to digital enterprises operating in the EU from external markets. In terms of regulatory models, the "adequacy determination" mechanism for cross-border data plays a role in reviewing the level of personal data protection in other countries. Shan Wenhua and Deng Na, Conflict, Coordination and Reference of Transborder Data Flow Regulation between the EU and the US: Comment on the "Schrems II" of CJEU, *Journal of Xi'an Jiaotong University (Social Sciences)*, No. 5, 2021, p. 94; Liu Jinrui, Towards Global Regulation of Cross-border Data Flows: Fundamental Concerns and the Chinese Approach, *Administrative Law Review*, No. 4, p. 75; Yuan hui, Mechanism Study on Adequacy Decision of EU Cross-border Transfer of Personal Data, *Electronics Intellectual Property*, No. 11, 2020.

7 Tian Xiaoping, EU General Data Protection Regulation from the Perspective of Trade Barriers, *Journal of Political Science and Law*, No. 4, 2019, p. 124.

8 United Nations Conference on Trade and Development, Digital Economy Report 2019 — Value Creation and Capture: Implications for Developing Countries, https://unctad.org/system/files/official-document/der2019_overview_ch.pdf (Last Visited on June 16, 2023); Xu Duoqi, International Pattern of Personal Data Cross-border Flow Regulation and China's Response, *Legal Forum*, No. 3, 2018, p. 131.

laws, and concludes with some useful suggestions.

II. SUPERVISION OF CROSS-BORDER DATA FLOW IN INTERNATIONAL RULES

There is no international data treaty that specifically regulates data flow, despite significant increases in cross-border data flows and varying regional regulatory obligations. Global data governance has become unpredictable as a result of the proliferation of domestic restrictions on cross-border data flow that have increased the compliance cost for businesses' cross-border operations and investments. In terms of the cessation of international collaboration and negotiations on cross-border data flows control, there are differing perspectives among nations about fragmented regulations.⁹ Countries differ in their approaches to data protection and their understanding of who owns personal information under their respective domestic legal systems. Similar terms like “data protection”, “privacy protection” or “data privacy” are frequently used to refer to legislative measures pertaining to the acquisition, use and storage of personal data, but they have diverse meanings and legal implications across different jurisdictions. The rapid expansion of the data economy and need for proper governance of the digital society has resulted in numerous regulatory difficulties that require countries to resolve them together through extensive collaboration.

Overall, the current lack of effective international governance for cross-border data flow is mainly manifested in the differences in regulatory objectives, a lack of regulatory consensus, and a weak foundation for international cooperation with regard to cross-border data flow, as well as the limited function and efficacy of regulatory coordination. All these factors are also the main reasons for the lack of international legal governance of cross-border data

9 Qi Junyan and Qiang Huajun, Data Flow Restrictions, Data Intensity and Digital Services Trade, *Modern Finance and Economics (Journal of Tianjin University of Finance and Economics)*, No. 7, 2022, pp. 3-4; United Nations Conference on Trade and Development, Digital Economy Report 2021 — Cross-border Data Flows and Development: For Whom the Data Flow, p. 8, https://unctad.org/system/files/official-document/der2021_en.pdf (Last Visited on June 16, 2023).

flow.¹⁰ There are also substantial variations in regulatory obligations when it comes to the types of data that is collected and the purposes for which they can be used or shared. The current international cross-border data flow regulation focuses primarily on personal data while management of other issues, such as the flow and circulation of non-personal data, remains in a nascent stage of development. It needs a faster evolution since its regulatory requirements are inadequate even when it comes to personal data governance.¹¹

With few exceptions, the General Agreement on Trade in Services (GATS) of the World Trade Organization (WTO) serves as the foundation for a multilateral model of governance. The WTO has been plagued by institutional flaws and a lack of updated rules in recent years. Its participation in negotiations has gotten worse; reforms have frequently been hindered; and the overall development of rules for digital trade has been sluggish. In addition to WTO regulations, international standards for cross-border data transmission can also be found in the institutional framework created by networks of bilateral and multinational free trade agreements.¹² The legal jurisdiction mechanism and management system standards for cross-border data flow that are broadly approved by countries have not yet been formalized within a framework of global governance.¹³

The principles and regulatory frameworks governing data flow and the protection of individual privacy are also included in the “soft law” norms in the field of international cooperation. It is impossible to ignore how soft law norms encourage cooperation. The following describes two aspects of this topic.

10 Xie Zhuojun and Yang Shudong, On the Regulations of Cross-border Data Flows in Global Governance and China's Participation: A Comparative Analysis Based on WTO, Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and RCEP, *International Review*, No. 5, pp. 105-106; Cai Cuihong and Wang Yuanzhi, Global Data Governance: Challenges and Approaches, *China International Studies*, No. 6, 2020, p. 44.

11 Wu Shenkuo, Global Trend of Data Governance and China's Countermeasures, *E-governance*, No. 1, 2019, pp. 6-7; Wang Rong, Cognition and Recommendations of Cross-border Data Flow Policies, *Information Security and Communications Privacy*, No. 3, 2018.

12 Xu Duoqi, The Construction of Trade Rule Framework that Governs Cross-border Data Flows, *Administrative Law Review*, No. 4, 2022, p. 51.

13 Huang Zhixiong (Ed.), *Legal Logic of Data Governance*, Wuhan University Press, 2021, pp. 492 & 495.

A. Supervision of Cross-border Data Flows under Multilateral Trade Agreements

Currently, two models are being proposed to promote the multilateral cooperation mechanism for data regulation: digital commerce rules and cross-border data flow efforts. Such regulation primarily relies on the establishment of provisions in regional, bilateral, and multilateral trade agreements linked to digital trade, cross-border service trade, e-commerce, and domestic laws pertaining to trade rules.¹⁴ It is worth mentioning that not all trade regulations that deal with or seek to limit cross-border data flow contain direct clauses pertaining to the same, meaning that they are not regulated by direct actions in cross-border data flow scenarios. In this regard, the academic community has widely examined how the “data sovereignty paradigm” of the EU or the more general “technology sovereignty” thesis affects the development of rules and judicial practice.¹⁵

In the current multilateral trading system, the content of trade norms for digital services is limited, and the distribution of terms is relatively dispersed. They are easily constrained by domestic regulations in actual commercial practice, making it difficult for them to perform a fundamental role in international governance. Against the backdrop of difficulties in the progression of WTO negotiations, various parties have explored and attempted to set up data regulatory cooperation among themselves. Other nations and regions can use these cooperation models formed as a guide. These models have highlighted several pressing challenges faced by national and regional legislation as well as the judiciary that must be addressed. Some believe that the regional regulatory system represented by the Regional Comprehensive Economic Partnership (RCEP)

14 For example, Chapter 9 of the EU Canada Free Trade Agreement covering cross-border trade in services, Chapter 15 covering telecommunications, Chapter 16 covering e-commerce, and Chapter 12 covering domestic regulations; Chapter 8 of the EU-Japan Free Trade Agreement (hereinafter referred to as the “EU-Japan Agreement”) on Trade in Services and E-commerce, Chapter 18 on Best Practices and Cooperation in Regulation.

15 Que Tianshu and Wang Ziyue, The Governance Paradigm of Cross-border Data Flow between the US and Europe and the Way Forward for China, *Journal of International Relations*, No. 6, 2021, p. 82; Liu Tianjiao, Theoretical Distinctions and Practical Conflicts between Data Sovereignty and Long-arm Jurisdiction, *Global Law Review*, No. 2, 2020; Quan Xiaolian, The Governance of Cross-border Data Flows in Trade Agreements: Is the CPTPP Framework an Ideal Way Out? *Frontiers of Law in China*, No. 15, 2020.

could better reflect the co-governance characteristics of cross-border data flow, particularly in accordance with the position and requirements of developing countries on data flow regulation issues. However, similar regional trade frameworks cannot take the place of an international legislation as they do not and may not provide unified and implementable global standards for cross-border data transfer.¹⁶

Some WTO members argue that limitations on cross-border data transfers are equivalent to barriers to international trade.¹⁷ According to Article 4 of the GATS Annex on Telecommunications, all member states must ensure that service providers from other member states can use public telecommunications transmission networks and services to send information within their own territory and across borders. In accordance with Article 5(4) of the Annex, member states may take necessary steps to ensure the security and confidentiality of information, provided that such steps are not implemented through discrimination that is arbitrary or unreasonable, or that masquerades as a restriction on trade in services. This article's paragraphs 5 and 6 outline many situations under which members are permitted to access and use public telecommunications transmission networks and services, as well as the rules for accessing and using public telecommunications transmission networks and services. Additionally, according to the GATS general exemption provision, member states are not prohibited from adopting necessary actions required to uphold public morality, maintain order, safeguard human, animal, and plant life, or preserve public health, among other things.¹⁸ Indeed, there is a chance that member nations' restrictions on the otherwise unrestricted flow of data across borders could, if they go beyond acceptable bounds, be considered arbitrary or unfair discrimination or amounting to veiled restrictions on trade under GATS regulations.

16 Xie Zhuojun and Yang Shudong, On the Regulations of Cross-border Data Flows in Global Governance and China's Participation: A Comparative Analysis Based on WTO, CPTPP and RCEP, *International Review*, No. 5, 2021, p. 104.

17 Zhu Fulin, The International Game of Digital Trade Rules, "Seeking for Common" Dilemma and China's Strategy, *Economic Review Journal*, No. 8, 2021, pp. 45-46.

18 GATS, Articles 4 and 5 of the Annex on Telecommunications, https://www.wto.org/english/docs_e/legal_e/26-gats_02_e.htm#anntel (Last Visited on June 16, 2023); GATS, Article 14, https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm (Last Visited on June 16, 2023).

However, at least on paper, the provisions of the GATS Annex on Telecommunications on service providers using networks for cross-border information transmission, the list of permissible restrictions and conditions for “access and use of public telecommunications transmission networks and services,” and the general GATS exception clauses collectively create a relative balance between the freedom of cross-border data transmission and national data security.

It is extremely challenging to come to an agreement on cross-border data flow standards under the auspices of the WTO in the current context. One reason for this is that the cross-border free flow of data in trade has not yet established itself as a cornerstone principle that is widely accepted by member states similar to the principle of “nondiscriminatory treatment”. Instead, it depends on each country’s market access policies and specific commitments made under the GATS regarding computers and related services. The other reason is that restrictions on the free flow of data across borders may contradict member nations’ national laws and regulations based on different definitions and standards of protection of personal privacy or personal information rights in different jurisdictions.¹⁹

The majority of the member countries are in the early stages of governing and regulating the free flow of data. Free trade agreements and regional trade agreements have developed into better platforms for collaboration and exploration in areas like services, investment, and intellectual property through economic cooperation and regulatory integration as compared to the WTO trade rules which are based on the principles of “reciprocity” and “non-discrimination.” They have lately taken center-stage in developed nations’ efforts to promote trade rule negotiations. The rapid development of regional, bilateral and multi-lateral trade agreement models can be attributed mostly to trade rule systems led by the United States and the EU. The US-Mexico-Canada Agreement and the US-Japan Digital Trade Agreement both adopt the “American-style template” pioneered by the USA.²⁰ The rules developed by the EU are more comprehensive

¹⁹ *Supra* n. 12, p. 52.

²⁰ Robert Holleyman, *Data Governance and Trade: The Asia-Pacific Leads the Way*, from the website of the National Bureau of Asian Research, <https://www.nbr.org/publication/data-governance-and-trade-the-asia-pacific-leads-the-way/> (Last Visited on June 16, 2023).

and binding than the “American-style template,” and they have stricter privacy protection requirements based on the “discourse of rights”. Even so, the European-style template is also inadequate.²¹ Articles 1 and 3 of Chapter 8 of the Euro-Japanese Agreement, for instance, specify the relative jurisdictions of the two parties with regard to trade in services, investment freedom, and e-commerce. According to Article 20 of the General Agreement on Tariffs and Trade, regulatory actions taken by one party may not result in arbitrary or unjust discrimination, or veiled restrictions on the services of the other party. Article 4 of Chapter 8 of the Euro-Japanese Agreement mandates the creation of a committee in charge of e-commerce, investment liberalization, and services trade. The sections pertaining to digital trade rules are not separate chapters and the provisions are rather dispersed.²²

B. Personal Privacy Protection under International Soft Law Norms

The majority of the international organizations with substantial impact and strong capabilities in the sector of trade and commerce are those that support international soft law regulations on cross-border data flow management.²³ In international law, legal standards are referred to as “soft law” if they have the potential to result in consequences even though they are not legally enforceable, do not create indefeasible rights or binding obligations and are not guaranteed to be implemented by the state.²⁴

It is uncertain how soft law regulations will evolve.²⁵ Its future development

21 Mira Burri, *The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation*, *UC Davis Law Review*, No. 51, 2017, pp. 85-90; Mira Burri, *Current and Emerging Trends in Disruptive Technologies: Implications for the Present and Future of EU's Trade Policy*, EP/EXPO/B/INTA/2017/06.

22 European Commission, *EU-Japan Agreement Chapter by Chapter*, https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/japan/eu-japan-agreement/eu-japan-agreement-chapter-chapter_en (Last Visited on June 16, 2023).

23 The term “soft law norms” in international law refers to voluntary, non-binding standards that are upheld by member states and take the form of guidelines, recommendations, judgments, standards, and best practices. Qi Tong, *The Validity of Soft International Finance Law and Its Development*, *Global Law Review*, No. 2, 2012, pp. 155-156.

24 Luo Haocai, *Treat Soft Law Seriously — The General Theory of Chinese Public Law and Practice in China*, *China Legal Science*, No. 2, 2006.

25 Liu Hongsong and Cheng Haiye, *Global Governance of Transborder Data Flow: Progress, Trends, and China's Path*, *Global Review*, No. 6, 2020, p. 69; Gong Yongqin and Wang Jian, *Comparison of Cross-border Privacy Rules of APEC and EU*, *Journal of Asia Pacific Economy*, No. 5, 2015.

is dependent on ongoing promotion and the creation of stringent legislation in order to ensure enforcement and implementation. The role of these regulations in resolving the issue of trade barriers is limited due to their emphasis on initiatives but lack of enforcement mechanisms.²⁶ There are also instances of conflict of rules. The concepts and rights protection advocated by soft law regulations are difficult to implement in practice if they conflict with other interests or rights protection requirements. Therefore, according to the rationalism school of international law, when there is a significant conflict of interest between countries, the development of cooperation and the design of systems must rely on hard law.²⁷

Formally, non-enforceable legal texts, such as initiatives to support the growth of the digital economy, as well as policies, guidelines and recommendations on privacy protection and international data flow, are included among the soft law norms related to the protection of individual privacy rights under international law. Adopted in 1980, the Organization for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and the Cross-border Flow of Personal Data is an example. This is the first international consultation-based guideline in the field of information privacy protection.²⁸ The Asia-Pacific Economic Cooperation (APEC) Privacy Framework, which was adopted in 2005, is another example. The framework aims to ensure that economies within the APEC zone can fully utilize the benefits of the development of the digital economy by creating relatively unified privacy protection and authentication standards, while avoiding the security risks associated with personal information protection and cross-border data flow. Targeting data controllers, a Cross-Border Privacy Rules (CBPR) data certification and

26 Hou Fuqiang, The International Trade Barrier and Its Legal Countermeasures Based on the Personal Information Protection, *Legal Forum*, No. 3, 2015, p. 40.

27 Xu Chongli, Global Governance and Transnational Legal Systems: The Construction of the "Center Peripheral" of Hard Law and Soft Law, *Foreign Theoretical Trends*, No. 8, 2013, p. 22; C. A. Whytock, A Rational Design Theory of Transgovernmentalism: The Case of EU-US Merger Review Cooperation, *Boston University International Law Journal*, No. 23, 2005, pp. 20-29.

28 Ao Haijing, Data Protection through International Soft Law, *Studies in Law and Business*, No. 2, 2022, p. 158.

transmission system rule has been formulated within this framework.²⁹ There are three stages of certification in the CBPR system: economic entity certification, responsible agency certification, and organizational certification. Currently, nine countries and regions are participating within this system, including Japan, the United States of America, South Korea, and Canada, but China is not one of them.

III. CROSS-BORDER DATA FLOW REGULATION IN THE EU-EVOLUTION AND CONTROVERSY

In the absence of a unified international codification, the domestic legislation and regional rule-making governing data flows between sovereign states have an effect on the business of multinational corporations providing digital services from external markets, resulting in actual exercise of long-arm jurisdiction, and even the creation of new barriers to digital trade.³⁰ Recent legislations enacted by the EU are prime examples.

The General Data Protection Regulation (GDPR), the Regulations on the Free Movement of Non-Personal Data, the Open Data Directive, and the Digital Content Directive are among the EU's many data protection legislation. This article discusses three new pieces of legislation: the Data Act, the Digital Services Act, and the Digital Market Act. The GDPR, which went into effect in 2016, replaced the previous fundamental law in the field of personal data

29 See APEC, APEC Privacy Framework, 2015, [https://www.apec.org/docs/default-source/publications/2017/8/apec-privacy-framework-\(2015\)/217_ecsg_2015-apec-privacy-framework.pdf?sfvrsn=1fe93b6b_1](https://www.apec.org/docs/default-source/publications/2017/8/apec-privacy-framework-(2015)/217_ecsg_2015-apec-privacy-framework.pdf?sfvrsn=1fe93b6b_1) (Last Visited on June 16 2023); OECD, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, In OECD, *the OECD Privacy Framework*, OECD Publishing, 2013, <https://www.oecd-ilibrary.org/docserver/9789264196391-en.pdf?expires=1686879717&id=id&accname=guest&checksum=6624C7F3282281E0CEBE1F65E4B8D2F9> (Last Visited on June 16, 2023); Clare Sullivan, EU GDPR or APEC CBPR? A Comparative Analysis of the EU and APEC to Cross Border Data Transfers and Protection of Personal Data in the IoT Era, *International Journal of Technology Law and Practice*, No. 35, 2019, pp. 380-397.

30 For example, in terms of basic concepts, the interpretation of the concepts of "data controller" and "data processor" in the Data Protection Directive and the GDPR is not limited to application within the EU region, but equally applies to digital enterprises within the EU and in external markets. In terms of regulatory models, the "adequacy determination" mechanism for cross-border data plays a role in reviewing the level of personal data protection in other countries.

protection, i.e., the 1995 Data Protection Directive. In addition to highlighting the EU's priority and planning on digital legislation, the digital development strategy documents released and updated over the past few years have also strengthened the rights of data subjects.³¹ The EU has developed a model for regulating the cross-border flow of data based on the defense of fundamental rights and the use of judicial review by the European Court of Justice as a regulatory tool.³² The EU's proposal on digital governance for 2020 contains two bills: the Digital Services Act and the Digital Markets Act.³³ The former primarily focuses on digital platform antitrust, whereas the latter mostly focuses on digital content governance. The two proposals seek to strengthen the EU's internal market.

A. Process of EU Data Governance Reform

The 1995 Data Protection Directive is the fundamental regulation for the protection of personal information in the EU. The Directive emphasizes that any behavior involving the processing of personal information must be regulated in principle, and that regulation cannot be an excuse to obstruct the free flow of information. This is important in terms of both the protection of personal information and the free flow of information. The EU Judicial Commissioner proposed data protection reforms in 2012. The foundation of the reform is the incompatibility of the present regulatory structures with the fast-expanding global data flow. Nearly all EU enterprises send data beyond the EU, but the Data Protection Directive's provisions on cross-border flows, which serve as the EU's institutional framework for cross-border data transmission, are challenging to adjust to the international flow of data.³⁴ To this end, the EU has reformed the

31 Jiang Ge, On the Model of a Personal Data Protection Act: A Study based on the German Experience, *Science of Law — Northwest University of Political & Law*, No. 2, 2011.

32 Jin Jing, EU Standard for International Transfers of Personal Data: Construction of Rules, Promotion of Justice and Expansion of Paradigm, *Chinese Journal of European Studies*, No. 4, 2021, p. 89.

33 Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and Amending Directive 2000/31/EC, COM/2020/825 final; Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act), COM/2020/842 final.

34 Fang Fang, The Evolution of EU Personal Data Cross-Border Flow Policy: Market Unification and Trade Norms, *Fudan International Studies Review*, Vol. 24.

management of data transfer through the GDPR. It specifically forbids member states from managing cross-border data flows in a licensed manner, adds object types for adequacy determination, expands standard contract terms to give businesses more options for cross-border personal data transmission contract text that suit their needs, and takes up the duties of third-party supervision and market self-discipline, such as industry associations.

GDPR is one of the EU's data protection regulations. The regulation establish the principles of legality, fairness, transparency, purpose limitation, data minimization, accuracy, limited retention, completeness, confidentiality, and seven fundamental norms of responsibility. Chapter 5 of the GDPR primarily reflects the legal obligations imposed by the EU for the purposes of governing international data transmission. Due to the concepts of personal and territorial jurisdiction, as well as international jurisdiction, the GDPR's area of application can be expanded to a global scale. Through GDPR, the EU strictly regulates data transmission, taking into account a number of factors, including actively controlling the ability to create cross-border data flow rules, reducing the digital power disparity between the US and Europe, preserving EU digital sovereignty, and more fully protecting fundamental rights like EU citizens' privacy rights. Some legal mechanisms, such as Standard Contractual Clauses (SCCs) and adequacy determination decisions, have been developed by GDPR.

According to some recent scholarly analysis, the protection of "data rights" as a fundamental human right serves as the legal foundation for EU GDPR data regulation. Some academics also believe that the GDPR emphasizes the protection of data subject rights. This legislation is consistent with the legal and cultural orientation of the EU, but it aims to apply the values and principles of human rights protection to achieve pragmatic economic objectives. Its principal goal is to govern the single digital market, and economic drivers are critical for understanding the EU's policy on cross-border data flows.³⁵ This article argues that the GDPR reflects the coordination of economic interests and the preservation of citizens' data rights in EU data legislation.

35 Ye Kairu, "Long-arm Jurisdiction" in Data Flow Regulation: Originalist Study on GDPR of EU, *Law Review*, Vol. 1, 2020.

Although the legislation launched in 2012 was led by the judiciary, according to official documents, the goal of EU's present reform is not solely intended to safeguard consumers' rights to privacy or data protection. Considerations that are more urgent include establishing a "single data market" and encouraging the growth and security of the EU's data sector. Data protection reform has been included in the measures to create a single digital market, rather than being intended for the protection of judicial and fundamental rights, according to the EU Commission's document on the 2016 work plan.³⁶

B. Controversy over EU Legislation and Justice

The 1995 Data Protection Directive was replaced by the General Data Protection Regulation (GDPR) after it was adopted in 2018. The recently updated digital development strategy document emphasizes the EU's agenda on digital legislation and overall planning, thereby strengthening the rights of data subjects.³⁷ The EU has developed a model for regulating the cross-border flow of data based on the defense of fundamental rights and the use of judicial review by the European Court of Justice as a regulatory tool.³⁸ The Digital Services Act and the Digital Markets Act are two measures that are part of the 2020 proposal for digital governance. Both are intended to improve the EU's internal market and partially reclaim "digital sovereignty".³⁹ The former primarily focuses on digital content governance, whereas the latter mostly focuses on digital platform antitrust. The EU establishes its regulations for digital services through stringent legislation, oversight, and enforcement procedures.

European digital service businesses are unable to compete due to EU digital legislation. The laws governing data in the United States, Japan, Singapore, and China have been significantly impacted by the regulations developed and put into effect by the EU in the context of digital reform. Due to tight review procedures and diverse impacts, they have also caused controversy. GDPR is a

36 European Commission, Joint Statement on the Final Adoption of the New EU Rules for Personal Data Protection, April 14, 2016. <https://ec.europa.eu/newsroom/just/items/30856> (Last Visited on June 16, 2023).

37 *Supra* n. 31.

38 *Supra* n. 32.

39 *Supra* n. 33.

crucial component of the EU's agenda for building a unified data market and data security as part of the EU's data protection reform initiatives. Previously, the data regulatory cooperation of United States has focused on cross-border data flow regulations only. The GDPR outlines the procedures and requirements for cross-border data transmission within the EU, including exemptions from restrictions on cross-border data transfer based on adequate protection recognition, transmission based on adequate protection of data subject rights and effective legal remedies, binding corporate rules (BCR) within multinational enterprises, and cross-border transmission allowed based on specific factors, such as public interest.⁴⁰

The data transfer system is now significantly more unpredictable as a result of stricter monitoring of judicial authorities. Its dispute resolution process has drawn a lot of flak since, in addition to being laborious, it also necessitates cross-border cooperation, which makes litigation challenging. Because of the "one-stop mechanism" it advocates, numerous data protection organizations in various nations must work together. The application procedure is uniform for businesses inside the EU as well as for businesses outside the EU that offer data services inside the EU. The EU indirectly controls cross-border data flow by verifying whether or not the recipient's level of data protection complies with the rules, rather than actively interfering with it. However, because of the uneven development of digital services and the disparities in regulatory frameworks among nations, American businesses are primarily affected in judicial practice, which has also led to institutional gaming between the two sides.⁴¹ Due to its stringent review processes and sanctions, GDPR has resulted in significant compliance costs for data giants from non-EU member states, particularly US data giants like Google. The GDPR regulations lack clear directions and are complicated in terms of compliance obligations, which creates uncertainty about the applicable standards.⁴²

The European Court of Justice nullified the Privacy Shield Agreement for

40 Chapter 5 of GDPR, <https://gdpr.eu/tag/chapter-5/> (Last Visited on June 16, 2023).

41 Gao Wei, New Public Utility Theory of Platform Regulation, *Chinese Journal of Law*, No. 3, 2021, p. 99.

42 *Supra* n. 15, Quan Xiaolian (2020), p. 272.

failing to adequately protect the privacy of European individuals, and the SCC model also ran into some difficulties. The European Court and the Irish High Court have declared the European and American Privacy Shield Agreement to be invalid, in addition to the extra compliance costs that GDPR has generated for external corporations expanding into Europe.⁴³ The SCC model apparently cannot be used to sustain data transfers between the EU and the United States, as the Irish Data Protection Commission ordered Facebook to halt the transfer of user data from the EU to the US in August, 2020. The primary justification given by the EU Court for invalidating the Privacy Shield Agreement is that the legal limitations on public access to data under US domestic legislation do not correspond to those in the EU. Under impact of this case, other EU member states may also make equivalent amendments and require Facebook to localize and keep data in Europe if the SCC model cannot serve as the legal foundation for cross-border data transmission between Europe and America. The strain on businesses that rely on cross-border data transmission between Europe and America in order to deliver digital goods and services, owing to increased compliance costs, has been reduced as a result of the replacement of the SCC model with a new framework.

In March, 2022, a new Trans-Atlantic Data Privacy Framework was published by the USA and the EU. The United States will put new safeguards in place to ensure the necessity and proportionality of information intelligence surveillance activities in pursuit of national security goals, as well as reforms to address the issues raised by the European Court of Justice in its *Schrems II* decision in July, 2020.⁴⁴ Previously, there were clauses pertaining to administrative authorities in the Privacy Shield Agreement between the United States and Europe. According to the agreement, the US government must make sure that its administrative agencies have clear limitations on their powers, and regulatory frameworks for their work upholding the law, for preserving national security,

⁴³ *Supra* n. 6, Shan Wenhua and Deng Na (2021).

⁴⁴ FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework, Statements and Releases, Briefing Room of the White House, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/> (Last Visited on June 16, 2023).

and defending social welfare.⁴⁵

IV. NEW TRENDS IN EU CROSS-BORDER DATA FLOW RULES

By tackling concerns including cybersecurity, platform accountability, market dominance, online advertising, electronic contracts, and online services, the EU is seeking to provide an environment of fair market competition for the internal internet market. The protection of individual privacy rights and the EU's overall security considerations are the cherished principles and legal norms that restrict the free flow of data, according to the process of EU data legislative reforms and changes in laws. China and the EU have essentially the same positions on the balance between civil rights and general security, as well as the free flow of data, in their respective legal systems. In the present wave of EU legislation, special consideration should be given to the design of review procedures and specialized requirements for digital service providers. In order to avoid disputes over digital trade barriers, China should take note of the EU's gradual but targeted approach to data-related legislations, the relationship between specific field legislation and high-level laws, and the best ways to strictly enforce requirements, strengthen supervision of data use, and increase transparency.

From the General Data Protection Regulation to the Data Act proposed by the European Commission, as well as the Digital Services Act and Digital Markets Act ultimately adopted by Europe in 2022, the focus of EU legislation has shifted from internal market unification to enhancing the management of internet platform enterprises. While maintaining the fundamental principles of personal data protection, current EU data legislation has added regulations in respect of several fields. Objectives of the EU can be seen from both the Digital Services Act and the Digital Markets Act, which include forming a unified single

45 Liu Biqu, Comment on "Privacy Shield Agreement" between the US and the EU, *Chinese Review of International Law*, No. 6, 2016, p. 38.

market, increasing confidence among consumers and small and medium-sized enterprises. The “data sovereignty” notion underpins EU legislation, which indirectly safeguards data subjects’ rights while not directly interfering with the flow and processing of data across international borders.⁴⁶ It contributes to the regulation of international digital trade and improves the long-term jurisdictional impact of its legislations by changing the jurisdiction to achieve non-discriminatory management of platform firms.

The new legislation’s weaker protection of individual privacy rights has, in some ways, boosted its ability to regulate trade and the legitimacy of some of its special laws. Prior to developing rules for specific trade industries, one must first complete the creation of the institutional infrastructure and the general legal framework. China can use the “two-step” concept of the EU’s cross-border data flow regulatory legislation as a model.

A. Expansion of Regulations

The EU Data Law (Draft) is a piece of legislation that proposes new standards of how non-personal data should be used. It is proposed to be applied to data produced by various intelligent devices and automated industrial processes. In addition to encouraging the openness of the data market and clarifying the obligations on data processing service providers, it intends to establish a framework for equitable access and sharing. Large internet platforms are required to comply with the bill’s requirements, which include sharing a lot of the commercial and industrial data they control during the review phase and adhering to a number of limitations on their ability to benefit from provisions on user data portability.⁴⁷ The standards of the review procedure are uniform in terms of fairness, regardless of whether the company maintains data in Europe or in the nation of origin, stemming the debate regarding the imbalance between internal and external market competition laws.

⁴⁶ *Supra* n. 15, Liu Tianjiao (2020), p. 186.

⁴⁷ European Commission, Proposal for a Regulation of the European Parliament and the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act), <https://op.europa.eu/en/publication-detail/-/publication/2c5d30ae-961f-11ec-b4e4-01aa75ed71a1/language-en/format-PDF> (Last Visited on June 16, 2023).

At the same time, the bill includes provisions and exemptions to safeguard small and medium-sized businesses from unfair contract clauses put forth by a powerful party in order to increase their competitiveness in data sharing negotiations in EU member states, and stop large corporations from abusing data sharing contracts. The Data Law (Draft) also contains special provisions for the cross-border flow of non-personal data that are just as strict as those contained in the GDPR. Most notably, several businesses are included within the bill's scope of applicability, including all manufacturers and suppliers of related services that sell goods in the EU market as well as consumers of these services, data owners who transfer their data to recipients in the EU, EU data recipients who receive data from data holders, data holders who provide data in response to requests from public sector organizations, data holders who provide data in response to requests from such organizations, data holders who offer data to EU data recipients, and suppliers of data processing services that offer these services to EU clients.⁴⁸ The obligation is primarily expressed by the necessity that businesses, as data exporters, will be required to confirm that the legal status of third countries complies with EU law and offer an adequate degree of data protection before engaging in commercial operations that result in cross-border data flow. If they do not meet the requirements, standard contract terms must be added.⁴⁹

B. Promote Fair Competition in the Digital Market

The European Parliament, the European Commission, and the European Council reached an agreement regarding the future implementation of the Digital Markets Act, which had already received support from member states, and issued a statement in March, 2022, prior to the passage of two new laws by EU legislators. They decided to use the law as a basis to impose restrictions on several technology giants, such as Google and Apple Inc.⁵⁰ The regulation governs

48 Lyu Na, The "One Body, Two Standards" Approach to Data Flow Governance in the EU Data Act, https://www.thepaper.cn/newsDetail_forward_16656846 (Last Visited on June 16, 2023).

49 *Supra* n. 32, p. 107.

50 The European Union Has Reached An Agreement on the Digital Markets Act, and Technology Giants Will be Restricted, http://www.news.cn/world/2022-03/25/c_1128503179.htm (Last Visited on June 16, 2023).

online intermediary service providers in the EU, such as internet access companies, domain name registrars, hosting companies, and online marketplaces, app stores, and social media websites. The law mandates internet platforms to adopt open data access policies and other particular regulatory measures. Large internet platforms are required to have risk management strategies, and those that don't comply risk a fine of up to 6% of annual sales.

According to this regulation, the European Digital Services Commission serves as a communication and liaison body while the EU member states are the primary regulatory organizations. The European Commission is in charge of enforcing and supervising large internet platforms.⁵¹ It is anticipated that numerous multinational internet corporations shall be subjected to supervision as a result of giving the European Commission enforcement authority to check on how major internet companies are complying with 21 new competition laws.

The opposition to the regulation is primarily focused on three issues: firstly, the law is not sufficiently detailed, and the European Commission should develop and issue guidance documents to assist “keeper” firms in complying with the law's provisions; secondly, the coordination of EU member states' competition law regulations; thirdly, the indistinguishable enterprise regulations may not meet regulatory requirements in practice. The European Commission must engage in discussions with gatekeeper businesses and adopt some supervisory measures that are appropriate for the business models of the companies involved when it comes to the privacy and security characteristics of various data platforms.⁵²

The Digital Markets Act includes more precise and acceptable standards for the objects of review in terms of openness, public obligations, and other

51 Cang Lan and Zhang Shucui, Looking at Platform Economy Anti-Monopoly from the EU's Digital Services Law and Digital Market Law, *Journal of Data Economy*, No. 6, 2021.

52 Wu Shenkuo and Hu Ran, The EU's New Scheme for Digital Platform Regulation and China's Experience: Analysis of the Proposal around the Digital Services Act and the Digital Markets Act, *Egovernance*, No. 2, 2021, p. 115; Matthias Leistner, The Commission's Vision for Europe's Digital Future: Proposals for Data Governance Act, the Digital Markets Act and the Digital Services Act — A Critical Primer, *Journal of Intellectual Property Law & Practice*, No. 16, 2021, pp. 778-784; Catarina Martins and Christophe Carugati, Insights for Successful Enforcement of Europe's Digital Markets Act, <https://www.bruegel.org/2022/05/insights-for-successful-enforcement-of-europes-digital-markets-act/> (Last Visited on June 16, 2023).

responsibilities compared to the criteria for the adequacy determination in the GDPR. The Digital Markets Act is a specialized legislation that targets businesses engaged in providing digital services in the particular sectors under consideration. It does not directly regulate the use and processing of EU data by external digital service enterprises, but instead innovates digital content governance based on the provisions of the previous E-commerce Directive. It categorizes digital services and requires online platforms with over 45 million users to actively review, process, and promptly delete illegal content such as false information and terrorist remarks. It also requires the platform to mandatorily check for any potentially harmful or fake third-party items, and make the advertising and ranking algorithms public. The maximum fine for violators is 6% of their annual revenue. According to enterprise regulations, higher standards are needed when it comes to pushing information, delivering advertising, and protecting minors. It oversees specific business sectors and is helpful for addressing unfair competition in the digital market from the perspectives of managing the EU internal market, preventing unfair competition, and protecting consumer rights.⁵³

C. Strengthen Platform Enterprise Responsibility

The primary regulations contained in the Digital Services Act pertain to online platform reporting obligations, third-party content responsibilities, and user security.⁵⁴ The Digital Services Act outlines the obligations of digital service providers to address the risks to users' privacy rights. The law is also committed to establishing a competitive environment that is fair, transparent, and orderly for both small and large platform businesses. Regarding data flow, the law prohibits only four measures that restrict cross-border data flow while maintaining high standards for personal information protection. The EU proposal is comprehensive and calls for the basic elimination of national treatment and market access restrictions when it comes to market access for telecom services.

53 Fang Yingxin, EU Legislation Strengthening Digital Regulation, <http://money.people.com.cn/n1/2021/0105/c42877-31988905.html> (Last Visited on June 16, 2023).

54 *Supra* n. 5, Li Shigang and Bao Dingyurui (2021).

Following the law's adoption, a report from the EU evaluated a number of factors that will contribute to its successful implementation, including:

a. There is a lack of specialized EU legislations protecting the rights of data users, despite the fact that custodian corporations have extensive control over data;

b. The formation of a “notification procedure” is mandated by Article 14 of the new law; however, there are no guidelines or specific provisions for doing so;

c. Regarding dispute resolution, there are currently no consistent norms at the EU level for digital services litigation, which costs consumers a long time to appeal as well as substantial legal costs;

d. In terms of jurisdiction, a large number of platform operators, particularly internet corporations with the largest market share in the EU, do not have their headquarters in the EU. Typically, contracts between traders within the EU and these platform businesses include a choice of jurisdiction and a choice of courts referring to the jurisdiction of the seat of the platform operator, resulting in the inapplicability of EU law in private international law matters.⁵⁵

V. ANALYSIS AND SUGGESTIONS FOR THE CURRENT SITUATION OF DATA LEGISLATION IN CHINA

The notions that might be at odds with the free flow of data from the standpoint of value assessment include, at the very least, personal privacy, national security, and emerging concept of personal ownership of data. How does the EU interpret and strike a balance between fundamental rights of individuals, regional security, and economic interests while regulating the free flow of data under the GDPR, and subsequently the Digital Markets Act, the Digital Services Act and the proposed Digital Act. This is a question worthy of further examination.

⁵⁵ Niomo Lomba and Tatjana Evas, Digital Services Act, European Added Value Assessment, *European Parliamentary Research Service*, 2020, pp. 13-15.

A. Comparison between the Basic Data Legislations of China and Europe

The fundamental legal framework for data security and personal information protection in China has essentially been completed with the passage of the Data Security Law and the Personal Information Protection Law in 2021. Both the EU and China have implemented a thorough legislative strategy to control data flow, with a focus on the protection of rights during the processing of personal data. The effects of GDPR on the entire global digital trade sector and inside the EU market differ significantly. It harmonizes and standardizes the European data market, strengthens the EU's influence in world affairs by utilizing market norms established among its member states. In particular, it makes use of the "adequacy determination mechanism" to assess the level of data protection in non-EU nations, thereby extending the regulatory authority of EU over international data based on market access requirements.

In terms of legislative values, the EU prioritizes human rights and the broader protection of rights, whereas China places a greater emphasis on tackling data security challenges brought on by digital trends. The Cybersecurity Law, for instance, specifies network information security issues and prescribes data management obligations for network operators. In contrast to the EU and China, the United States lacks a comprehensive data protection law, as the foundation for its data protection relies mostly on industrial autonomy and administrative enforcement by the private sector to protect personal privacy. However, in order to guarantee exclusive jurisdiction and restrict the outflow of domestic data, the United States has embraced the principle of territorial jurisdiction within its legal framework. With its market advantages, the Clarification of the Legitimate Use of Overseas Data Act establishes the standards for data controllers and extends the long-arm jurisdiction of the state to any data market in which the United States participates.

B. Recommendations for Data Rules in China

At present, China's data legislation is fragmented. Personal information protection

laws, national security laws, and data management laws and policy documents are drafted independently. It is hereby advised to take into account the higher-order legal definition of “power” as the value when processing data, as opposed to the legislative model of the EU, and to improve data protection standards through supporting measures, implementation techniques, and so on, in order to avoid potential conflicts of laws during application in judicial practice. In terms of cross-border data flow and market access for telecom services, China’s E-commerce Law and the EU’s Digital Services Act can be in conflict.⁵⁶

The application of new standards in laws and regulations, like “personal information protection” and “data outflow regulations”, should be incorporated into subsequent trade legislation through revisions and amendments. In terms of e-commerce-related services, cloud computing services are an extremely open and sensitive field. Future legislation may take one of three approaches: data legislation unification and integration, digital services trade legislation, or the incorporation of data processing-related content in the three capital laws and foreign trade laws, or a separate legislation for digital services trade.

In terms of rights protection, the new highlight of China’s Personal Information Protection Law is the special obligations on internet platforms, the strengthening of the obligations of personal information processors, and the clarification of the various rights of individuals in personal information processing activities. Based on China’s current situation and international experience, the Personal Information Protection Law establishes the principles that should be followed when processing personal information, emphasizing that personal information processing should be based on the principles of legality, legitimacy, necessity, and integrity; the objective must be to minimize the impact on personal rights and take adequate safety measures.

Currently, China’s framework for cross-border data flow categorizes regu-

56 China Outsourcing Institute, Impact Analysis and Countermeasure Suggestions of the European Union’s Digital Services Law, <http://www.coi.org.cn/article/bt/u/202008/20200802991442.shtml> (Last Visited on June 16, 2023); Wu Shenkuo, What Are the Inspirations of the EU Digital Services Law on the Governance of Chinese Internet Platforms, <http://tech.hexun.com/2022-04-26/205818434.html> (Last Visited on June 16, 2023).

lated objects as either personal data or essential data. In the future, China should not rely solely on data outflow security assessment as a compliance mechanism in order to maximize the contribution of digital elements to economic development. Instead, we can take inspiration from the EU's experience and adopt a "diversified" flow mechanism, which includes establishing a whitelist mechanism, adhering to the main standards of security assessment, establishing a guiding model for cross-border data flow agreements, and encouraging industry associations and other self-regulatory organizations to participate in security assessments. We can also implement classification management methods for different datasets. Regarding cross-border data flow compliance, emphasis should be placed on the goal and severity of cross-border data flow policies, as well as potential problems like unfair competition. Chinese data platform businesses with a worldwide development strategy must blend globalization and localization philosophies to address the challenges brought on by the current territorial disputes between nations and regions. In this regard, the EU regulation does not require data localization explicitly, and businesses outside the EU are theoretically free to transfer data via a variety of channels.

As a developing country, China is now unable to regulate exports in the same manner as developed countries do in the WTO multilateral discussions and negotiations for bilateral, multilateral, and regional trade agreements. In order to respond to new developments in the field of digital trade and e-commerce, it should take into account the search for a community of parties with common interests to form a negotiation group, support and promote the WTO's reform, and encourage multilateral negotiations between developed and developing countries on regulatory integration.⁵⁷ China should also value the benefits and potential function of soft law norms. In comparison to rigid hard law norms, soft law is more adaptable, is more amenable to the actor's control as an additional commitment and empowerment, and has comparatively lower

57 Chen Huanqi, Convergence Trends in the Context of International Digital Trade Rules Game: Based on the Perspectives of China, the US and the EU, *International Business Research*, No. 3, 2022; Gao Jiang and Sheng Bin, Principles of Economics of WTO and FTAs: From Traditional Trade Rules to New Trade Rules, *International Economics and Trade Research*, No. 5, 2019, p. 19.

legislative costs.⁵⁸ Soft law norms can be used as a backup mechanism for the current system of international governance of cross-border data flow in the absence of a universally recognized system of rules, preventing potential illegal infringement of rights as a result of technological development, thereby safeguarding public interests.

⁵⁸ *Supra* n. 16, Xie Zhuojun and Yang Shudong (2021), pp. 113-114.