Woody International Publish Limited
An Multidisciplinary Academic Journal Publisher

Journal of Theory and Practice of Humanities Science, Volume 2, Issue 2, 2025
https://www.woodyinternational.com/

The Study on Exception Clauses of Cross-Border Data Flows in International Trade Agreements

Qi Sun

The University of Melbourne, Melbourne, Victoria, Australia

Abstract: ***This article mainly tells about the definition and characteristics of cross-border data flows, and analyzes different governance models by using comparative methods, for example, it lists America, EU and China's governance models, because each economy entity represents the different model. The international agreement was signed by many countries, and different countries have their own governance models due to different considerations. So in the international agreement, it has different exception clauses lies in various international trade agreements. And these agreements can be divided into the WTO Agreements and other regional agreements. According to the comparison methodology, this article analyzes the common application dilemmas and thus promotes the construction of an international order for cross-border data flow.***

Keywords: Cross-border data flow; Digital Economy; Exception clauses.

Cited as: Sun, Q. (2025). The Study on Exception Clauses of Cross-Border Data Flows in International Trade Agreements. *Journal of Theory and Practice in Humanities and Social Sciences*, *2*(2), 1–18. Retrieved from https://woodyinternational.com/index.php/jtphss/article/view/177.

1. An overview of cross-border data flows

The cross-border flow of data appeared due to the combination of globalization, digitalization and cross-border cooperation.[1] Firstly, as for globalization, it not only contains local resources but also integrate data resources and operations through global value chains. Secondly, the rise of new technology has provided the method to store data and process data more flexible, which store data in other country's data centers for training in order to serve the local consumers better. Thirdly, as for cross-border cooperation, many international organizations and corporations have the demand and make an effort in sharing information resources for collaboration, such as United Nations databases. The three forces gather together, providing the opportunity for cross-border data flows.

1.1 Definition of Cross-Border Data Flows

In 1984, the report by the United Nations Centre on Transnational Corporations puts forward the definition of cross-border data flows. However, at that time, the term of 'cross-border data flows' hasn't been created, similarly, it has the definition of "trans-border data flows" it interpreted TBDF as the movement of data across national borders.[2] However, this definition is universe, in the new Ages, many scholars and different organizations have variable views. Scholar Eric J. Novotny thinks it is units of information for processing by one or more digital facilities which transfer or process the information in more than one nation-state.[3] This definition emphasizes the working mechanism of data flows; However, scholar Milton Mueller uses the comparative method to define it. Under the economy theory, factor mobility is a substitute for trading goods across borders',[4] so under the context of trading across borders, cross-border data flows defined is the mobile factor of digital trade. However, these definitions are too narrow because they can't cover all the fields. In addition, the organization WTO views cross-

[1] Lusine Vardanyan & Hovsep Kocharyan, 'Critical views on the phenomenon of EU digital sovereignty through the prism of global data governance reality: main obstacles and challenges' (2022) 9 (2) *European Studies* 110.
[2] United Nations Centre on Transnational Corporations, *Transnational corporations and transborder data flows; a technical paper* (1982).
[3] Branscomb, Anne W, 'Global Governance of Global Networks: A Survey of Transborder Data Flow in Transition.' (1983) 36 *Vand. L. Rev. 36* 985.
[4] Mueller, Milton and Grindal, Karl, '*Is It Trade?' Data Flows and the Digital Economy* (Report, August 2018) 1.

border data flows as 'a key element supporting international trade and e-commerce,[5] involving data exchange through the internet.'

According to author's opinion, it should be identified under the context of international economic law, and the definition should reflect the nature of it. So it can be defined as 'the movement of data between countries or regions under their different legal and technical frameworks through digital networks, which supports the global digital economy.'

1.2 Characteristics of Cross-border Data Flows

According to the common theory, there are three significant characteristics about data flows: transnational, electronic and diversity.[6] According to author's opinion, these characteristics can be interpreted as flexibility and diversity.

Firstly, flexibility means technology transportation flexibility and geographic flexibility. The technology transportation flexibility means it can be transmitted through wired technologies (fiber optics) or wireless methods (Wifi), replacing physical infrastructure. The geographic flexibility means that data can break the geography limits and data can flow across different regions or countries.[7]

On the one hand, diversity is expressed in the diverse pathways, on the other hand, it also be expressed in multiple data types. As for the pathways, cross-border data flows are unidirectional, bidirectional or even multidimensional. Businesses may need to acquire data from multiple countries or store data across various data centers in different nations. In addition, cross-border data flows involve various types of data, ranging from traditional text information, images, as well as machine learning models and artificial intelligence algorithms.

2. Different Governance Models of Cross-border Data Flows

Different countries have their own special governance models of cross-border data flows due to different economy level and digital economy level. These models can be reflected by different countries' legislation and practice. There are three typical cross-border data regulatory governance models. The first model is the free model, and it is represented by the United States. The second model is represented by the European Union and China, and they have the interventionist model. The third model is data localism model represented by Russia.

Firstly, as for the 'free model',[8] in a word, it means data flows liberalization. U.S. emphasizes the principle of limited government's participation in the cross-border data flows, and promotes the level of free flow of data. The United States has always been dominated by the free flow of data, to capture more digital resources internationally while weakening the strength of competitors.

And this 'free model' focuses on the 'free'. The 'free' can be reflected in market access and trade agreements. As for market access, the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA)[9] established market access rules for industries involved in cross-border data, especially the data which may affect the flow and use of cross-border data. FIRRMA argued that if the involved company handles or collects sensitive personal data of U.S. citizens, CFIUS can initiate a review based on this.

As for the trade agreements, the United States officially implemented the USMCA on January 29, 2020.[10] The principles of rules is 'data freedom', no party can create impose unnecessary obstacles towards cross-border data flows. In addition, it also requires the openness of government data. In the Biden administration, the U.S. promoted "data liberalism" and stipulates regulation requirements including the total prohibition of data transmission

[5] Mitchell, Andrew D., and Neha Mishra. 'Regulating cross-border data flows in a data-driven world: how WTO Law can contribute.' (2019) *Journal of International Economic Law* 22 (3) 389.
[6] Mitchell, Andrew D., and Neha Mishra. 'Regulating cross-border data flows in a data-driven world: how WTO Law can contribute.' (2019) *Journal of International Economic Law* 22 (3) 389.
[7] Ibid.
[8] Aaronson, Susan Ariel, 'Data is disruptive: How data sovereignty is challenging data governance.' *Hinrich Foundation* (2021).
[9] U.S. Congress. the Foreign Investment Risk Review Modernization Act of 2018[EB/OL]. (2018-08-13) [2021-11-29].
[10] Donald J. Trump. Continuation of the National Emergency with Respect to Securing the Information and Communications Technology and Services Supply Chain[EB/OL]. (2020-05-14) [2022-11-29] https://www.federalregister.gov/documents/2020/05/14/2020-10594/continuation-of-the-national-emergency-with-respect-to-securing-the-information-and-communications.

restrictions and localization measures.[11]

So this kind of model is contrary to the EU, the EU's overall model prioritizes privacy interests. Scholar Joel R. Reidenberg puts forward the theory that it should protect privacy, and it can't pursue economy interests at the cost of damaging privacy. That's also the principle of EU's governance model. So the European Union established the regulation General Data Protection Regulation (GDPR), which passed in 2016 to protect every EU citizen's privacy. It has the implementation tools,[12] which includes three main mechanisms: "Adequacy Decisions," "Appropriate Safeguards," and "Derogations for Specific Situations.[13] As for non-personal data, recent laws have the rules the Data Governance Act (DGA).[14] And the public sector or service providers, as well as data organizations can be covered by the DGA. It contains a series of technical or legal measures to prevent such cross-border obstacles.

Another example of interventionist model is China. Chinese governance model means that Chinese government will play the role in intervening the free flows of cross-border data under proper purpose, and protects personal information.[15] In China, in 2021, China passed The Personal Information Protection Law (PIPL), establishing strict regulations for the cross-border transfer of personal information, it implies that personal data must comply with one of the four legal mechanisms before transferring data abroad.[16] According to the Article 38 of the PIPL, the four compliance pathways include: the first pathway is Security Assessment by the Cyberspace Administration of China (CAC).[17] It can be applied to large-scale personal information, sensitive personal information of over 100,000 individuals and critical Information Infrastructure Operators (CIIOs), it can conduct a security assessment, including reviewing the necessity of the data transfer, the security capabilities of the overseas recipient and the potential risks to national security or public interest.

The third governance model is Russia's data localism model. According to Data Localization Law, Russia requires nearly prohibits the cross-border privacy data flows and it must stay locally.[18] And the governance model is out of the consideration of national security.

National security is the fundamental foundation for a country's survival. If a country's security is threatened, it may face political damage, economic recession, or even the risk of war. In modern society, the concept of security has expanded beyond traditional personal and property security to include information security, cybersecurity, and data security. Under the context of cross-border data flows, data security has become a part of national security. And the misuse of data will cause potential risks for data security, and thus cause damage for national security.

In 2013, due to the influence of the Prism Gate incident in the United States, Russia began to pass legislation requiring Russian users to store data on domestic servers for local storage and backup.[19] First, in 2016, Russia amended Law of the Russian Federation on Communications, requiring all operators to store user data in local data centers in Russia.[20] At the same time, operators are required to set up their own data centers in the country, and co-hosting schemes are not recognized. In the next few years, operators should migrate 70% of their data to data centers in Russia. In addition, In accordance with the Law on Personal Data, when collecting personal data from domestic and foreign companies, the data collector is obliged to ensure that the personal data of citizens of the Russian Federation are recorded, organized, accumulated, stored, updated and extracted using databases located on the territory of the Russian Federation. Even if a company operates online and does not have a physical presence in Russia, the company must comply with the requirements of this law as long as its activities are directed at Russian citizens.[21] According to the Law on Personal Data, companies can entrust the storage and processing

[11] Stephen Bartholomeusz. Digital trade war: Biden opens new front in effort to contain China[DB/OL](2021-09-01)[2021-10-13].
[12] European Commission. A European Strategy for Data[EB/OL]. (2020-02-19)[2022-12-06]. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN.
[13] Article 46. General Data Protection Regulation[Z/OL]. Intersoft Consulting Homepage(2016-05-04)[2022-12-06]. https://gdpr-info.eu.
[14] European Commission. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)[EB/OL].(2022-06-03)[2022-12-06].
[15] Zheng, Weiwei. "Comparative Study on the Legal Regulation of a Cross-Border Flow of Personal Data and Its Inspiration to China." Frontiers L. China 15 (2020): 280.
[16] Calzada, Igor. "Citizens' data privacy in China: The state of the art of the Personal Information Protection Law (PIPL)." Smart Cities 5.3 (2022): 1129-1150.
[17] Liu, Junchao. "China's Security Assessment Measures for Outbound Data Transfers." JE Asia & Int'l L. 16 (2023): 267.
[18] Russian Data Protection Laws: Essential Guide on Compliance Requirements in Russia, at https://incountry.com, March19, 2021.
[19] Savelyev, Alexander. "Russia's new personal data localization regulations: A step forward or a self-imposed sanction?." Computer law & security review 32.1 (2016): 128-145.
[20] Medvedev, Sergey. "Data protection in russian federation: overview." Thomson Reuters Practical Law (2016).
[21] Ibid.

of restricted data to third parties, provided that the cloud service provider's data center is located in Russia. Personal data can also be transferred abroad for processing, however, a copy must first be stored on a server physically located on Russian territory. When choosing a cloud service, choose those certified providers that store and protect Russian citizens' personal data in accordance with the Russian Law on Personal Data Protection.

3. The Current Situations of International Rules in Regulating Cross-border Data Flows

3.1 Fragmentation of international rules on cross-border data flows

Just as mentioned before, cross-border data flows is accessible and flexible, when data flows cross borders, so it is necessary to develop a set of international rules that can be applied to the world. In recent years, different rules of cross-border data flow creates unnecessary trade barriers when data flows cross borders, This means that the extent to which different countries' laws and regulations restrict cross-border data flows varies, which causes obstacles in cross-border data flows. It is not conducive to digital economy. Nowadays, the international agreements are centered on the WTO agreements. However, firstly, under the WTO framework, there are the GATT and GATS agreement, GATT is mainly for trade in goods, and GATS is mainly for trade in services. It is still difficult to define whether digital products embodied in special forms such as data should be classified as goods or services. Secondly, it is lack of special and systematic legislation to deal with current cross-border data flows. Some scholars put forward to use former Internet rules to regulate cross-border data flows, but they are not very proper to act as the international rules and the number are not sufficient.

3.2 The international rules on cross-border data flow are distinctly differentiated

Due to the current global harmonization of international rules for cross-border data flow, the policies and regulations between countries are also different due to national interests and cultural differences, and the regulating objective is different. Thus, different countries have different standards for balancing national security and data flow. This means that the extent to which different countries' laws and regulations restrict cross-border data flows varies. And this variation can be reflected in a number of bilateral and regional free trade agreements for cross-border data flows between regional economies or countries for the need for cross-border data flows. The most significant two are APEC and OECD.

Firstly, APEC's Cross-Border Privacy Rules (CBPR) is a voluntary framework aimed at providing a unified data protection standard for APEC member economies, The core goal of the APEC framework is to promote cross-border data flow, particularly in the Asia-Pacific region.[22] APEC places great emphasis on the development of digital trade, believing that the liberalization of data flow is crucial for promoting regional economic growth. Therefore, APEC emphasizes the freedom and flexibility of data flow when promoting data protection.[23]

However, the OECD Privacy Guidelines established the core principles of data privacy protection in global data governance, particularly emphasizing the need for privacy protection in cross-border data flows.[24] The OECD Privacy Guidelines explicitly require countries to establish adequate privacy protection mechanisms when promoting cross-border data flows, ensuring the security of personal data.[25] The OECD advocates for the establishment of a globally consistent data protection standard, but this does not mean that all countries must enact identical laws. Instead, it suggests that countries adopt measures that are coordinated and compatible, reducing legal differences in data protection between countries and facilitating cross-border data flows.

4. An Overview for International Trade Agreement Exceptions Clauses in Cross-border Data Flows

Exception clauses are a compromise way to balance free flows of cross-border data and national regulatory authority in trade agreements. From the agreement GATT/WTO system to the TPP and CPTTP, one of the common

[22] Singh, Seema. "Regulation of Cross-Border Data Flow and Its Privacy in the Digital Era." NUJS J. Regul. Stud. 9 (2024): 38.
[23] Tan, Johanna G. "A comparative study of the APEC privacy framework-a new voice in the data protection dialogue?." Asian journal of comparative law 3 (2008): 1-44.
[24] Mattoo, Aaditya, and Joshua P. Meltzer. "International Data Flows and Privacy." Development Research (2018).
[25] Ibid.

features of these international trade agreements is that they all set certain exceptions to them in certain ways. And these exception clauses maintains the stability, sustainability and flexibility of the treaty system

4.1 The History and Definition of Exceptions Clauses in International Trade Agreement of Cross-border Data Flows

Many trade agreements contain clauses to deal with change in cross-border data flows, they also contain provisions of balancing of interests, which provide special protections of particular policies in their own country. From the perspective of nature, many scholars argued that exception clauses can be defined as the specific clauses in international trade agreements where certain goods, services, or actions are allowed to be exempt from certain provisions of the agreement.

Similarly, according to author's opinion, it refers to exception clauses in cross-border data flows refers to provisions within international trade agreements' regulatory frameworks, which aims to balance the need for data protection with the need for international trade.

The history of exception clauses in international trade agreement can be traced back to early Friendship, Commerce and Navigation (FCN) Treaties.[26] This pattern that consists of including exception situations in trade agreements firstly appeared. After that, the "exception clause" was first mentioned in the reciprocal trade agreement between the United States and Mexico, and the "exception clause" was again mentioned in the 1945 Trade Agreements.[27] It has been followed in several hundred bilateral and regional trade treaties which emerged since that. The establishment of GATT (General Agreement on Tariffs and Trade) in 1947 marked the beginning of the establishment of the exception clauses in the global trade system.[28] During this period were structurally established. Within the GATT framework, although free trade was the primary goal, the diverse economic structures, cultural backgrounds, and political needs of different countries fostered exception clauses. Article 19 of the GATT is the example of significant exception clauses. According to Article 1 of the GATT, if a country's domestic law conflicts with Part II of the GATT Principles of Substance, then the provision will be considered a special legal regime, known as a "grandfather clause".[29] The purpose of the "grandfather clause" is to coordinate between the autonomy of the parties and the fulfillment of the obligations under the agreement, and it can be said that it is the prototype of the exception clause in international trade agreements. The GATT exception allows countries to sanction products that are deemed to be detrimental to the industrial development with which they compete. If the harm comes from an equal deal with, then a government may invoke exceptions to control it.

After that, in 1995, World Trade Organization (WTO) marked a significant transformation in the global trade system. The WTO not only inherited the GATT framework but also modernized global trade rules by introducing new areas and issues, including services trade. GATS (General Agreement on Trade in Services) is the agreement within the WTO framework specifically addressing services trade, and Article XIV of GATS provides exceptions allowing member countries to implement certain measures in services trade. Similar to Article XX of GATT, GATS also allows countries to take restrictive measures in cases of public health crises or cultural protection. Countries can restrict or control the cross-border flow of certain services based on national security needs. These provisions enable countries to protect their specific public interests while liberalizing trade, especially in areas such as national security, public order, cultural protection, and public health.

With the development of digital economy and the establish of domestic governance models, international trade agreements related to regulating cross-border data flows also rise.

Trans-Pacific Partnership (TPP) agreement in 2016 is the first agreement which have binding exception clauses of

[26] Galagan, Dmytro. "The First Bilateral Investment Treaties: US Postwar Friendship, Commerce, and Navigation Treaties." (2017): 646.
[27] Yoo, Ji Yeong, and Dukgeun Ahn. "Security exceptions in the WTO system: bridge or bottle-neck for trade and security?." Journal of International Economic Law 19.2 (2016): 417-444.
[28] Ibid.
[29] Desta, Melaku Geboye. "The Law on International Trade in Agricultural Products: From GATT 1947 to the WTO Agreement on Agriculture." (2002): 1-486.

cross-border data flow in the e-commerce chapter. [30] And it can be reflected in chapter 14, and the content focuses on electronic commerce, including cross-border data transfers and the forced localization of computing facilities.[31] Just as mentioned, the 'binding' means each TPP member states should allow the cross-border transfer of information by electronic means. The exception clauses has the pre-condition 'to achieve a legitimate public policy objective', that means only under this objective, it can adopt or maintain a measure inconsistent with this obligation. Bur the measure "does not impose restrictions on transfers of information greater than are required to achieve the objective".[32]

TPP has become a model for later international trade agreements, not only fully preserved in the 2018 Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) agreement but also provides the sample for the 2020's United States–Mexico–Canada Agreement (USMCA).

4.2 The importance of International Trade Agreement Exceptions Clauses in Cross-border Data Flows

International Trade agreement Exception clauses maintains stability and sustainability of legal framework. The international trade agreement of Cross-border data flows develops with the reform of society, so that means the international trade agreement should change consistently with the society, however, there are some unexpected situations or some new needs, including protecting private privacy, protecting national security, etc. So if trade agreement cannot adapt to technological changes, their enforceability will be less effective. Secondly, from the perspective of state's obligation, Exception clauses do not arbitrarily allow countries to evade trade obligations; rather, they established pre-established legal mechanisms that can be cited under specific circumstances, ensuring that member states can be exempted from liability when exercising their exception rights, this can avoid frequent changes and maintain stability.

As for sustainability, the global trade system may face major shocks such as economic crises. Without exception clauses, many countries might unilaterally terminate agreements or withdraw from the trade system, severely undermining the continuity of legal frameworks. Exception clauses provide countries with a legitimate space for policy adjustments, ensuring that agreements remain effective during crises. From the perspective of dispute settlement, international trade disputes are inevitable, but if the legal system lacks sufficient flexibility, such disputes could lead countries to withdraw from agreements or resort to retaliatory measures. Exception clauses offer a predictable legal basis, allowing countries to defend their actions within a lawful framework, thereby enhancing the sustainability of the dispute resolution mechanism.

International Trade agreement Exception clauses maintains flexibility. The mechanism of action for balancing differences in the exception clause is to regulate the design of its specific rules, and to set relaxed or strict conditions for its application, specific or broad language, to regulate the extent to which its regulatory purpose can be achieved, and in essence, to regulate the discretion of countries to impose restrictions on cross-border data flows, as well as the scope of restrictions stipulated in the exception clause. Firstly, countries still seek to maintain a degree of policy autonomy in certain key areas in international trade agreement, such as national security, public health, and moral order. Exception clauses provide a mechanism to balance national sovereignty and international commitments, allowing countries to adopt policies that align with their national interests in specific circumstances without being deemed in violation of international rules. For example, in 2015, the United States revised the TPP-related rules on cross-border data flows, Paragraph 2 of Article 14.11, which permits cross-border data, including private data, and for legitimate public policy purposes listed in paragraph 3, authorizes the person concerned to perform or maintain an action inconsistent with paragraph 2 in order to achieve his or her legitimate public policy purpose, subject to two restrictions. With regard to the non-mandatory localization of data storage, the first paragraph of TPP 14.13 clarifies the need for control based on the security and confidentiality of communications in the countries concerned, and Article 14.13(3) affirms the principle that data localization is not regulated, except for legitimate public policy purposes, with the applicable qualifications in Article 14.11.

[30] Azmi, Ida Madieha Abdul Ghani, and Jeong Chun Phuoc. "INTERNATIONAL NORMS IN REGULATING ECOMMERCE: THE ELECTRONIC COMMERCE CHAPTER OF THE COMPREHENSIVE TRANS-PACIFIC PARTNERSHIP AGREEMENT." International Journal of Business & Society 21 (2020).
[31] Ibid 32.
[32] Wolfe, Robert. "Learning about digital trade: Privacy and E-commerce in CETA and TPP." World Trade Review 18.S1 (2019): S63-S84.

5. Analysis of the Application of the WTO General Exception Clauses related to Cross-border Data Flows

There are many general exception rules in WTO system, including GATT and GATS. And for each of them, according to the scholar Petros, exception rules are divided into business exceptions, non-business exceptions, and institutional exceptions.[33] Specifically, commercial exceptions include anti-dumping measures, safeguard measures, etc.; Non-commercial exceptions include general and security exceptions;[34] Institutional exceptions address exceptions such as special and differential treatment. So this part mainly tells about the non-commercial exceptions--- general and security exceptions.

5.1 An Overview for the application of the GATT General Exception Rule

GATT (General Agreement on Tariffs and Trade) is a multilateral international agreement that aims to promote international trade, reduce trade barriers, and provide a fair trading framework for countries. It was signed in 1947 and replaced by the World Trade Organization (WTO) in 1995. Nevertheless, the principles of GATT are still carried forward within the WTO framework.[35]

GATT general exception rules can be reflected in the article XX. And the article XX include three thresholds: firstly, the objective of the measure conforms to the objectives in the article XX. Secondly, the measure must satisfies the 'necessary' standard; thirdly, the measure must satisfies the chapeau test in the article XX. All the three conditions are regulated in the one paragraph. Panels and appealing bodies will normally consider each threshold in the following order, only if the previous threshold is met, the next threshold can move on.

5.1.1 Whether the measure conforms to the objective in Article XX

Article XX lists 10 possible exceptions, some of the most common ones include: XX(a) necessary to protect public morals ; XX(b) necessary to protect human…… life or health; XX(d) necessary to secure compliance with laws and regulations which are not inconsistent with the provisions of this Agreement; XX(g) relating to the conservation of exhaustible natural resources. For example, in the case EC – Asbestos (EU Asbestos Case, 2001), the EU banned the import of products containing asbestos to protect workers and consumers from the health risks caused by asbestos, because they argued it may cause lung cancer and asbestosis. Canada filed a complaint, arguing that the ban violated GATT rules, specifically the principles of national treatment (NT) and most-favored-nation (MFN). So the EU relied on the Article XX(b) protection of health exception to argue that asbestos is so harmful to human health that an import ban is necessary. Asbestos is scientifically proven to cause serious health hazards, so the goal of the measure is justified .

5.1.2 Assess whether the necessity standard is met for certain exceptions to Article 20

In Article 20 of GATT, the "necessity" standard is an important legal concept, which requires that the measures taken by member countries must cause as little damage to international trade as possible while achieving their public policy goals. The "necessity" standard involves the following aspects:

Although the exceptions provided for in Article 20 of the GATT allow member states to take trade restrictive measures in certain circumstances, such measures must meet certain conditions, especially the "necessity" standard. The assessment of the necessity standard includes several standards. First, the WTO will consider the importance and urgency of the policy objective. If the policy objective involves major issues related to public welfare such as life and health, environmental protection, etc., the "necessity" standard of the measure will be more relaxed. Secondly, the WTO will assess whether there are other alternative measures that can achieve the same policy goals with less trade disruption. If there are milder measures that can effectively achieve the goals without causing too much trade restrictions, the WTO may consider that the original measures do not meet the "necessity" standard. Thirdly, the effectiveness of the measure is also taken into account. The WTO examines whether the measure is effective in achieving its intended objectives without creating excessive barriers to trade.

[33] Petros C. Mavroidis, The General Agreement on Tariffs and Trade: A Commentary, Oxford University, 2005.
[34] Ibid.
[35] Shukla, Surya Pal. "From GATT to WTO and Beyond." (2000).

Thirdly, if there are Analysis of Chapeau Requirements. Even if a measure qualifies for one of the exceptions in Article 20, it still needs to pass the Chapeau Clause. The Chapeau Clause requires that the measure not constitute arbitrary or unjustifiable discrimination, nor be a disguised restriction on trade.

Assess whether the measure applies different standards to different countries and whether it is discriminatory. The chapeau of Article 20 contains three additional levels of tests for policy measures. These three are: (a) the measure "applied in a manner that does not constitute a means of arbitrary discrimination against States in the same condition"; (b) the measure is "applied in a manner that does not constitute a means of unjustified discrimination against States in the same condition"; (c) the measure is "applied in a manner that does not constitute a disguised restriction on international trade"

5.2 Application of General Exceptions in GATS

Under the institutional framework of the WTO, measures on cross-border data flows are more likely to be taken under the General Agreement on Trade in Services (GATS). Because exception clauses in GATS mainly focuses on the services, and data flows is closely linked to cross-border trade in services. So GATS is more closely related to data flows among the WTO rules. So the general exceptions in GATS can also be applied in the cross-border data flows area.

The general exception to GATS Article 14 is based on GATT Article 20, and they are applied in similar methods. GATS Article 14 allows Member States to derogate from their market access and national treatment commitments in order to take the necessary measures to protect interests. It provides a more detailed list of exceptions to trade commitments. Paragraphs (a) to (e) set out different exceptions with different standards. Paragraphs (a), (b) and (c) require that the measure be "necessary" to achieve its policy objectives. Paragraphs (a) and (c) are always wildly applied.

For example, in paragraph (a), this requires that the challenged measure relate to the specific interest in the provision and that there is a sufficient link between the measure and the protected interest. The connection is limited by qualifiers such as "necessary". Second, if the challenged measure is found to be an interest under Article 14, it will also need to be examined whether the measure satisfies the requirements set out in the chapeau to this article. The group of experts in question also considered that the content of these concepts could vary in space and time, and that members had the right to decide on the level of protection they considered appropriate. The understanding of "public order" also needs to be carried out in conjunction with GATS footnote 5, that is, the maintenance of the fundamental interests of society as reflected in public policies and laws. According to the Commentary, the public order exception under the general exception clause may only be invoked if there is a real and serious threat to the fundamental interests of society.

Second, conduct a "necessity" test. The criterion of "necessity" set out in the general exception clause is objective. the Appellate Body believed that the following three points should be taken into account: first, the concept of "necessity" reflects the importance of the object to which the actions are taken and is the focus of common values. The more important the common good or value, the more likely it is that the action will be defined as "necessary". Second, the review of "necessity" should take into account the extent to which the action achieves its objectives, and if the action achieves the stated objectives to a large extent, then the action can easily be considered "necessary". Consideration should be given not only to the existence of less restrictive and more moderate trade measures, but also to the effectiveness of alternative measures in achieving the stated objectives. Third, it is necessary to consider whether there are alternative measures, i.e., whether there are policies or measures that are less restrictive in trade. It is necessary to consider not only whether there are less restrictive and milder trade measures, but also whether alternative measures can effectively achieve the stated objectives. Finally, there is a need to review whether the requirements of the chapeau to this article have been met, i.e., that the measure in question must not constitute "arbitrary or unreasonable discrimination" or "disguised restriction on trade in services". This provision has been interpreted by the WTO's adjudicating bodies as an open normative model designed to prevent members from abusing the exception clause on the basis of whether the measure meets the requirement of "consistency".

5.3 Analysis of GATS general exceptions for cross-border data flows

It can be seen that the data is relevant under paragraphs (a) and (c) (ii) and (iii) (1) of paragraphs (a) and (c) of the GATS in accordance with Article 14 of GATS. Because (a) and (c) are exceptions to public morality and public order and protecting privacy, this is consistent with different countries' restriction measures.

As for the paragraphs (a), the member needs to determine its definition of "public morality" or "public order". At present, neither the panel nor the Appellate Body has made an authoritative conclusion to these two concepts for the time being, and has given members greater autonomy in determining what constitutes "public morality" and how measures to "protect public morality" are determined. Compared with the judgment of "public morality", the judgment of "public order" is stricter and limited to "the protection of basic social interests". However, this paragraph still gives members room to use the clause to defend against restrictions on the flow of data. They argued that cross-border data includes sensitive data, such as government data, military secrets, and important infrastructure information. If such data is stored or transmitted abroad without supervision, it may threaten national security and public order. Cross-border data is necessary to public order.

With regard to subparagraphs (ii) and (iii) of paragraph (c), subparagraph (ii) reads: "..... (ii) the protection of the privacy of individuals in connection with the processing and dissemination of personal information and the protection of the confidentiality of personal records and accounts.....", in this place, "Security" here should specifically refer to "the security of personal information and personal privacy". So when the states has the considerations of protecting individual privacy or the security of personal information, if other members lodge a complaint against these restrictive measures, the member imposing the restrictive measures may consider invoking subparagraphs (ii) and (iii) of paragraph (c) for defense.

In addition, it also needs to prove that the restrictive measures imposed by it are necessary to comply with domestic regulations. If the member is able to pass the necessity test, then it will consider whether there is a reasonably feasible alternative with less trade restrictions. Finally, it is also necessary to examine whether its restrictive measures on cross-border data flows meet the requirements of the preamble, that means whether the restrictive measures are implemented in good faith, and whether there is no arbitrary or unreasonable discrimination, and do not constitute disguised trade restrictions.

As privacy protection is one of the considerations set out in state's governance model, for restricting cross-border data flows, it is closely linked to the provisions of Article 14(c) (ii). Therefore, it is feasible for cross-border data flows to be reviewed under the GATS Article 14 General Exception.

6. Analysis of WTO security exception rules applicable to cross-border data flows

6.1 Analysis of WTO security exception clauses in general situations

Cross-border data flows is closely linked to national security, so there is a high likelihood that States will invoke security exceptions as a defense. As part of exception clauses, national security exception clauses are politically sensitive. Security exception clauses in international treaties usually adopt an enumerative approach, that is, they clearly list several situations in which countries can take security exception measures under specific circumstances, rather than an inductive approach (that is, providing an abstract concept and allowing countries to freely interpret the scope of application).

WTO security exception is reflected in GATS Article 14, generally speaking, traditional security exemptions include five categories: (1) national security information, (2) military installations, (3) nuclear fission, etc., nuclear fusion material, (4) war or international emergency, and (5) United Nations obligations.[36]

As for the application of WTO security exceptions, the key question is whether and to what extent GATT Article 21 is self-judging.[37] A self-adjudication clause is a clause in which a state may unilaterally depart from or derogate from its obligations after subjective assessment of the use and invocation of the clause. Just as mentioned, in

[36] Jiang, Chengze. "Research on Applying the WTO Security Exception Clause to the Security Dispute Caused by Cross-border Data Flows." 2021 International Conference on Social Development and Media Communication (SDMC 2021). Atlantis Press, 2022.
[37] Chen, Tsai-fang. "To judge the" self-judging" security exception under the GATT 1994-A systematic approach." Asian J. WTO & Int'l Health L & Pol'y 12 (2017): 311.

subparagraph (b) in security exception clause, it uses ‘ It considers’, that means it gives member states a broad "right to self-determination",[38] in theory, They seek to allow members to advance certain national interests from a national perspective. But due to the ambiguity and sensitivity of its content, its application in practice is different. In practice, the WTO has resolved only two cases involving members' invocation of safeguard exceptions, namely DS512 and DS567.[39] In DS512, the Panel clarified firstly argued that this is not a matter of self-censorship under the security exception. It made it clear that the relevant measures taken under the security exception were subject to review. While respecting Member States' own assessments of their essential security interests, it retains its own power to conduct objective reviews. In DS567, the panel takes into account factors such as the principle of good faith, the principle of proportionality and influence on other countries, to determine whether the measure is necessary to protect ‘essential security interests’.

As for the definition of ‘essential security interests’, the definition of essential security interests is ambiguous, In the DS512 case, the panel held that the scope of basic security interests was narrower compared with security interests,[40] and it means, and it was up to the WTO members to make their own judgment on which situations were basic security interests in light of the actual situation. However, members should be constrained by the fundamental principle of international law of "good faith" in making judgments about their essential security interests, and members use security exceptions to circumvent their obligations or judge commercial interests as security interests.

Thirdly, as for the "war or other emergencies in international relations", it is one of the prerequisites for invoking the security exception, which determines the time at which the security exception applies.

The panel put forward that "emergency in international relations" is an objective fact, and it is up to the panel to judge whether the members meet the "emergency situation in war or international relations". Secondly, the panel provided a clear explanation of "emergency situations in international relations’. That means the degree of the emergency goes beyond the degree of general political tension between states.[41] The panel interprets the degree of ‘international relations emergency’ as with the degree of "war".

6.2 Analysis of WTO security exception rules applicable to cross-border data flows

As for the cross-border data flows, subparagraph (b) of GATS Article 14 is the most relevant security exception clause about the cross-border data flows. Despite the lack of a clear definition of digital trade regulation at the WTO, there has been a discussion on the interpretation of certain WTO rulings and GATS Council documents issued as part of the work plan on e-commerce. Cross-border data flows are a key part of digital trade, and the application of GATS rules for digital trade also has a binding effect on cross-border data flows. The general exception to GATS Article 14 is reasonable for restrictions on cross-border data flows.

Article 14-1(b) (i) of GATS may include restrictions on cross-border data flows related to digital services of military agencies. Subparagraph (ii) of paragraph (b) may include projects including nuclear fusion and restrictions on the cross-border flow of fission-related information. Subparagraph (iii) is broader in scope, and the term "war", if broadened to include cyber battlefields, is also an issue of restrictions on the cross-border flow of sensitive data, which involves a question of traditional and non-traditional security, whether these non-traditional security issues faced on the Internet should be set as a special exemption from security exceptions, and how to specify them in these sub-items so as to ensure both the free flow of data and the protection of data security.

7. Analysis of Exceptions to Cross-Border Data Flows in Free Trade Agreements

Nowadays, most current free trade agreements prohibit restricting the free flow of data across borders, but they

[38] Zhao, Shuo. "The Determination of “Basic Security Interests” in the WTO Security Exception Clause." Studies in Law and Justice 2.4 (2023): 92-100.
[39] Liang, Yong, and Zhijie Peng. "Empirical Evolution of the WTO Security Exceptions Clause and China’s Discourse." A Chinese Perspective on WTO Reform. Singapore: Springer Nature Singapore, 2023. 139-169.
[40] Yunpeng, Wang. "RECONCILING NATIONAL SECURITY REVIEW OVER CROSS-BORDER INVESTMENT BILATERALLY." Труды Института государства и права Российской академии наук 19.1 (2024): 190-231.
[41] Yoo, Ji Yeong, and Dukgeun Ahn. "Security exceptions in the WTO system: bridge or bottle-neck for trade and security?." Journal of International Economic Law 19.2 (2016): 417-444.

have different legislation in the exceptions rules. However, FTAs vary in the degree of restriction of their rules on cross-border data flow. According to the different degrees, these exceptions of FTAs can be divided into several categories, including: exceptions in CPTPP and USMCA which represents U.S.; exceptions in DEPA which represents Singapore; exceptions in RCEP which represents developing countries. Among these FTAs, the U.S.-Mexico-Canada Agreement (USMCA), it only sets up exceptions only for legitimate public policy objectives. Conversely, the Regional Comprehensive Economic Partnership (RCEP) provides broader scope for exceptions, not only includes regulatory exceptions and exceptions to legitimate public policy objectives, but also includes essential security interests exceptions.

7.1 The analysis of exception for cross-border data flows led by U.S.

The CPTPP and USMCA are typical U.S.-led FTAs, and the provisions on the free flow of cross-border data largely reflect the U.S. claims and intentions.

7.1.1 Specific Exceptions in the CPTPP

CPTPP can be traced back to the TPP, and become the successor of it.[42] Originally, the TPP was the first FTA to include binding provisions on cross-border data flows in the e-commerce chapter, and the CPTPP essentially retaining the provisions of TPP.[43]

The issue related to e-commerce in CPTPP lies in chapter 14, and it is consisted of 18 articles, covering a lot of topics, including personal information protection, cybersecurity rules, electronic transaction frameworks, etc. In the e-commerce part, it contains the regulatory exceptions and public policy exceptions.[44] Article 14.11.1 of the CPTPP provides for regulatory exceptions, although the CPTPP sets out the general principle of the free flow of data across borders, members may still take measures to restrict the electronic transfer of certain information of national security concerns due to domestic regulatory requirements.[45] Similarly, Article 14.13 of the CPTPP on the location of computing facilities also provides for a regulatory exception in paragraph 1,[46] which, unlike Article 14.11, adds a provision that "includes requirements to seek guarantees of the security and confidentiality of communications".

The public policy exception to the CPTPP is set out in Article 14.11.3. If Member States invoke public policy exceptions in their defences, the CPTPP dispute settlement mechanism will have to assess the "legitimacy" of the policy objectives,[47] which means that restrictions on cross-border data flows, such as privacy, must be applied indiscriminately within and outside the country for the purposes of legality requirements. And "Legitimacy" indicates that this threshold is relatively low and can address a wide range of policy objectives. In order to meet the requirements of this article, there are three conditions. Firstly, it does not constitute arbitrary or unreasonable or disguised discrimination, secondly, it does not exceed the necessary limits, thirdly, it is motivated by legitimate public policy objectives.

The USMCA is still a US-led FTA, and it follows the TPP template. The USMCA has changed the previous statement in the e-commerce chapter of the TPP and stipulated digital trade as the title of the chapter in Chapter 19.[48] Article 19.12 of the USMCA prohibits data localization, reflecting a bias towards liberalization in the location of data storage facilities.[49] Article 19.8 focuses on the protection of personal information, and Article

[42] Barradas, Roberto Zapata. "The TPP, a Horizontal Overview." The Comprehensive and Progressive Trans-Pacific Partnership: The Trans-Pacific Partnership, the Comprehensive and Progressive TPP, their Roots in NAFTA and Beyond (2021): 40.
[43] Ibid 45.
[44] Leblond, Patrick. "Uploading CPTPP and USMCA Provisions to the WTO's Digital Trade Negotiations Poses Challenges for National Data Regulation."
[45] Yoshinori, A., and Policy Research Institute, Ministry of Finance, Japan. "Data localization measures and international economic law: how do WTO and TPP/CPTPP disciplines apply to these measures." Public Policy Review 16.5 (2021): 1-29.
[46] Leblond, Patrick. "Uploading CPTPP and USMCA Provisions to the WTO's Digital Trade Negotiations Poses Challenges for National Data Regulation."
[47] Ibid.
[48] Burri, Mira. "Digital trade rulemaking in free trade agreements." Research Handbook on Digital Trade. Edward Elgar Publishing, 2023. 9-27.
[49] Ciuriak, Dan, and Robert Fay. "The USMCA and Mexico's prospects under the new North American trade regime." Chapter 2 (2021): 45-66.

19.10 mainly tells about the access and use of the data to regulate barriers restricting the flow of data.[50] Among these articles, they can be divided into two parts. The first part is the relevant provisions on cross-border data outflow, including articles 19-11, 19-12 and 19-8; the second part is the data inflow provisions on the free flow of data across borders, with articles 19-10 and 19-16.

In chapter 19, the exception clauses in USMCA of reflects on the three principles of free flow of cross-border data, prohibition of data localization and disclosure of government data. Article 19.11 of the USMCA deletes the provisions of Article 14.11 of the CPTPP on the provisions governing the contracting parties, and restricting the application of other countries in their own laws. That means it maintains the same public policy exception as the CPTPP in Article 19.11(2) only, and removes the regulatory exception in Article 19.11(1) that prohibits the cross-border transmission of information by electronic means.

In addition, Article 19.12 prohibits the localization of computer facilities, states that no party should establish or use a computer equipment as a condition of its operations in a country.[51] The company cannot be restricted by requiring the company to establish a data center locally, or requiring the company to use local facilities to do business. The USMCA does not set any exceptions to data storage localization, which fully reflects its attitude towards the complete prohibition of digital localization. This clause will greatly break down the "digital trade barriers" and promote the further flow of cross-border data. Compared with CPTPP, these provisions don't mention "Public Policy Exceptions" in data localization, but it provides in Annex 19-A that Article 32.1 (General Exceptions) is binding on Article 19.17 (Interactive Computer Services). In addition, Article (2) provides that Article 14(a)(b)(c) of GATS has been amended and included as part of it to impose some restrictions on the flow of data.

7.2 The analysis of exception Rules for cross-border data flows led by Singapore

The Digital Economy Partnership Agreement (DEPA) is a free trade agreement initiated by New Zealand, Chile and Singapore. It aims to set digital trade standards, enhance digital trade level, and strengthen support for small and medium-sized enterprises in the digital age.[52] And it covers a series of issues in the digital trade, including data governance and cross-border data flows, E-Payments and FinTech and AI regulations. On June 12, 2020, the signing ceremony of DEPA was held between the three countries, marking the birth of the world's first multilateral special economic and trade agreement.[53] It is a creative regional agreement that fills the gap in global digital trade rules. And its rules and framework provide an example for other countries and regions.

DEPA has established systematic exception rules, and these rules can be divided into the regulatory exceptions and exceptions to legitimate public policy objectives.

As for the regulatory exceptions, Article 4.3 of DEPA provides for the cross-border transfer of information by electronic means, and paragraph 1 provides a regulatory exception, noting that the agreement takes into account the fact that Member States may set their own regulatory requirements for the electronic transmission of information;

In addition, it also has the exceptions to legitimate public policy objectives. DEPA allows Contracting Parties to take necessary restrictive measures to safeguard public interests, including: protecting national security; maintaining public order; ensuring financial stability; protecting consumers and personal data and preventing fraud and criminal activities.

7.3 Exceptions Rules in cross-border data flows led by developing countries

7.3.1 The regulatory Exception Rules in RCEP

[50] Ibid 52.
[51] Del Giovane, Chiara, Janos Ferencz, and Javier López González. "The Nature, Evolution and Potential Implications of Data Localisation Measures." (2023).
[52] Lee, Joo Hyoung, and David Collins. "The Digital Economy Partnership Agreement (DEPA): accession to the digital-only regime." Research Handbook on Digital Trade. Edward Elgar Publishing, 2023. 90-101.
[53] Kalin, Roman Pascal. "The Emergence of Digital Trade Regulation." Digital Trade and Data Privacy: Cross-border Flows of Personal Data Between Data Protection and Data Protectionism. Cham: Springer Nature Switzerland, 2024. 67-155.

On January 1, 2022, the RCEP officially entered into force, with a total of 15 members. The RCEP also covers cross-border data flows, with Chapter 8 "Trade in Services" and Chapter 12 "Electronic Commerce" both addressing cross-border data flows.[54] The RCEP allows cross-border data flows within contracting parties, but strictly limits the cross-border flow of telecommunication information and financial information, and sets exceptions based on data security.

Article 14(1) and (2) of the RCEP provide for regulatory exceptions, which in principle allow for cross-border data flows to be transmitted by electronic means, and neither completely prohibit nor encourage the localized storage of data.[55] Article 1 of this Article states: 'The Parties recognize that each Party may have its own measures regarding the use or location of computing facilities, including the requirement to seek to ensure the security and confidentiality of communications." Article 2 provides: "The contracting parties shall not make the use of computing facilities located within their territory or the establishment of such facilities within their territory a condition for conducting business within their territory." In principle, the RCEP allows the cross-border transfer of information through electronic means for cross-border data flows, and neither completely prohibits nor encourages the localized storage of data. Article 15.1 is the regulatory exceptions rules, that means the Parties recognize that each Contracting Party may have their own regulatory requirements for the transmission of information by electronic means.[56]

7.3.2 The Exceptions to legitimate public policy objectives

Contracting Parties shall not prevent investors or service providers from transferring information electronically across borders for the purpose of conducting business. However, the exception is permitted if a Contracting Party considers that restrictive measures on the cross-border transfer of information by electronic means are necessary to achieve its legitimate public policy objectives and that the measures do not constitute unreasonable discrimination or disguised trade restrictions. This means that Parties can regulate cross-border transfers of information for fundamental national security interests or legitimate public policy objectives. Similarly, with regard to data delocalization, in the ordinary course of business activities, enterprises have the right to determine the location of their computing facilities, and a contracting party cannot force enterprises to remain in their national territory. However, if the location of the facility is outside the normal course of operations, poses a security concern to the contracting State, or changes the location of the computing facility for legitimate public policy purposes, a Contracting Party may impose a requirement on the location of the computing facility of an enterprise.

The RCEP's provisions on exceptions to legitimate public policy objectives reflect the RCEP's principle of data sovereignty in the governance of cross-border data flows.[57] It does not have a separate section on the exception to legitimate public policy objectives, but it does have an exception to legitimate public policy objectives in the chapter on e-commerce. The applicable provisions for legitimate public policy objectives can be reflected in Article 14 on the location of computing facilities in the promotion of cross-border electronic commerce and in Article 15 on the electronic transmission of cross-border information. Article 14 is mainly about location of computing facilities. DEPA prohibits parties from forcing companies to store data or establish computing facilities locally as a prerequisite for doing business in the country. However, the "legitimate public policy objectives" exception allows member states to set the following regulatory requirements. The first one is Data localization requirements, if it is to protect national security, public safety or personal data privacy. The second one is critical infrastructure regulation, if computing facilities involve key industries such as finance, medical care, energy, communications, etc. , member states can set compliance requirements. The third one is law enforcement compliance requirements, member states can require that some data must be stored locally so that law enforcement agencies can obtain information.

As for Article 15, in principle, RCEP prohibits the imposition of unnecessary restrictions on the cross-border

[54] Dayday, Czar Matthew Gerard T. "Cross-border data flows and data regulation under international trade law." Phil. LJ 96 (2023): 33.
[55] Chin, Yik-Chan, and Jingwu Zhao. "Governing cross-border data flows: International trade agreements and their limits." Laws 11.4 (2022): 63.
[56] Ibid 58.
[57] Zhai, Dusheng. "RCEP Rules on Cross-Border Data Flows: asian characteristics and implications for developing countries." Asia Pacific Law Review 33.1 (2025): 24-45.

transmission of information by electronic means.[58] Member States may not require that data must be stored locally or that it must not be transferred abroad without permission. However, the "legitimate public policy objectives" exception allows member states to set the following regulatory requirements: The first one is personal data protection. If cross-border data transmission may affect user privacy rights, member states can set compliance requirements (such as data encryption, user consent mechanism). The second one is financial and payment data supervision. For data involving banks and payment systems, member states can require that data be stored or processed within their borders. The third one is law enforcement and national security. If cross-border data flows may be used for Law enforcement and national security. If cross-border data flows may be used for terrorist activities, cybercrime or other illegal activities, member states can impose restrictions. The fourth one is Public health and biosecurity. When it comes to sensitive information such as medical and health data and genetic data, member states can set special cross-border transmission regulations .

8. The difficulties of applying exception clauses to international trade agreements

8.1 The rules for the interpretation of exception clauses are ambiguous

8.1.1The ambiguity of the definition of the term

The definitions of terms for cross-border data flows are ambiguous in trade agreements, that means there is no unified definition of term that can be recognized by all the member states in the agreement. The reason is that the definitions of public policy and regulatory objectives vary in different agreements. Specifically speaking, in the negotiation of the agreement, states have a strong incentive to interpret exceptions in a broader way than expected in order to conform to their own benefits. When more countries join an agreement, this definition is harder to be defined. Thus, many countries have tried to abuse these clauses to protect their own interests, and it will cause damages to the effectiveness of the agreement. For example, as for the ‘public order’, public order is generally associated with concepts such as social stability, political security, and cyberspace governance, but its definition remains broad. For example, some countries may restrict the cross-border flow of specific types of information, such as news media or social media platform data, under the pretext of "maintaining public order." In the field of data governance, certain countries may require data localization on the grounds of "public order risks." However, whether such requirements meet the necessity principle remains controversial. RCEP, in its E-Commerce Chapter, allows member states to implement exceptions based on "public order." However, it does not clearly define the scope of "public order," leading to significant differences in implementation standards among member states.

In addition, it also has the political reason, political control based on mutual benefit is preferred over legal regulation, and emergency security operations between States have long been largely regulated through consultation and informal dispute resolution bodies. It is believed that politics can play a greater role in regulating the security exceptions. As a result, disputes relating to this provision are usually dealt with through diplomatic channels and informal dispute resolution mechanisms. In the WTO era, the security exception was also often seen as a self-definite exclusion clause and was used as a defense against all WTO rules. The reason for this is that even though members freely join the WTO and are bound by the WTO, they still retain a certain degree of autonomy on sensitive policy issues. This is illustrated by the fact that the dispute settlement body has the power to interpret WTO rules, while WTO members have the power to define situations such as "security interests," "exigencies," and "necessity."

8.2 Ambiguity of the applicable rules

The scope of application in exception rules refers to the extent to which state members can reach rule exceptions in the agreement. The greater the scope of the exception clause, that means a provision provides too much flexibility for its members, it is easy to undermine the responsibilities of a treaty, and the enforcement of the exception rules are less useful. Conversely, in the absence of an exception clause, no agreement could be reached even with some flexibility in place.

However, in the absence of clear rules for the application of general exceptions, security exceptions and exceptions

[58] Huang, Gui, and Yin Lei. "The norms on cross-border data flows in the RCEP." Asian Journal of Law and Economics 13.3 (2023): 375-404.

to specific restrictions in various trade agreements, and how the order and manner in which the various exceptions are applied and invoked, the entire trade agreement needs to be reviewed and harmonized in this new era of rapid development of digital trade and personal data information. Under WTO rules, security exceptions (GATT Article 21) take precedence over general exceptions (GATT Article 20). However, in agreements such as RCEP and DEPA, it is not explicitly stated whether security exceptions have priority over general exceptions.

8.3 The Excessive burden of Proof

In the dispute settlement process, the respondent (usually the party implementing the trade restrictive measures) needs to provide sufficient evidence to prove that its measures are reasonable and pass the "necessity" or "proportionality" test. However, the process of providing evidence is strict. For example, in the necessary test, it has three measures. Firstly, measure whether the measure achieves legitimate policy objectives. Secondly, it should analyze whether the measure is "necessary", that is, whether there are other alternative measures that have less impact on trade but are equally effective. Thirdly, it should assess whether the trade restrictiveness of the measure is commensurate with its contribution to the policy objectives. During the test, firstly, to demonstrate that their measures are intended to achieve specific legitimate policy objectives, it requires scientific research, data analysis and expert opinions to achieve policy goals. Such evidence usually needs to be verified by internationally recognized organizations, such as the World Health Organization (WHO), the United Nations Environment Programme (UNEP), etc., otherwise it may be considered to lack authority. In the Brazil—Retreaded Tyres case, , the WTO Appellate Body required Brazil to provide detailed data analysis to prove that the import of retreaded tires would indeed lead to environmental degradation, rather than just theoretical speculation. As for alternative analysis, This suggests that if the respondent cannot prove that all possible alternatives are ineffective or unfeasible, its measures may be found to be illegal, in some degree, it not only requires the defendant to prove the rationality of its own measures, but also requires it to analyze all possible alternatives and refute them one by one. This undoubtedly greatly increases the complexity and workload of evidence.

Thirdly, the even if a measure passes the first two steps, it must still meet the proportionality test. The WTO adopts high standards for review, any situation where the data is not detailed enough, the evidence is not authoritative enough, or the argument is not rigorous enough may lead to a loss. This high standard of evidence requirement poses a challenge to many developing countries, as they may lack sufficient resources to conduct comprehensive scientific assessments.

8.4 Risk of discretionary abuse in exception clauses

The phrase "parties believe" that often appears in the exception clauses of various trade agreements. It gives Member States a great deal of freedom to recognize that they have more freedom to regulate cross-border data flows, which leads to the abuse, this clause appears to be an unrestricted evasion clause that allows members to exercise their discretion freely and with few restrictions.

The arbitrary measures taken by the States concerned to control cross-border data flows, taking advantage of the autonomy granted by this article, will not only make relations between States more chaotic, but also more fragmented in the world. It will be difficult to liberalize cross-border data flows if sovereign states are allowed to arbitrarily determine basic security interests in accordance with the discretion granted by the provisions, including the meaning and extension of cybersecurity interests, and then supervise and restrict cross-border data flows. It will be difficult to liberalize cross-border data flows if sovereign states are allowed to arbitrarily determine basic security interests, including the meaning and extension of cybersecurity interests, in accordance with the discretion granted by the provisions, and then supervise and restrict cross-border data flows. While legal restrictions is important, they are not the only way to prevent the abuse of exceptions, since the last choice is always in the hands of sovereign States.

9. The Solution to the Problem of the Application of Exceptions in international trade agreements

The solutions requires the international and domestic joint efforts. From the international efforts, it needs the clear

explanation of definition and application rules, decreasing the burden of proof in necessary and preventing discretionary abuse.

9.1 Suggestions for Improving Flow Exception Rules

9.1.1 Identify the connotation of the terms used in the exception clause

As for the security clauses, it can learn the application rules of WTO, in the WTO rules, although it doesn't contain the specific regulations of cross-border data, it can combine with the current exception clauses legislation in the international agreement related to cross-border data flows in order to adapt to the current cross-border data flows situations. Due to the consideration behind all kinds of exception clauses, it should modify the exception clauses according to the current situation. For example, as for clauses related to political sensitivity of national security issues, such as security exception clauses, member states can list the various situations in which an agreement is signed, leaving sufficient room for the interpretation and implementation of the provisions. Member States are able to interpret the term national security differently in different contexts, without being bound by the words of the treaty. Another example is 'pubic interests', nowadays, in the international agreement exception clauses, it doesn't imply the specific categories, and its aim is to protect a country's people's profits not be damaged, so public interests refers to the legitimate public policy objectives required to achieve the overall welfare and order of society, meanwhile, the public interests can't be achieved at the cost of damaging other country's interests.

In addition, while certain exceptions in trade agreements give parties considerable autonomy, they must consciously abide by the relevant rules set out in the Vienna Convention on the Law of Treaties (hereinafter referred to as "the Convention") when invoking these provisions. In order to prevent some Member States from safeguarding their own security and safeguarding the public interest, Articles 31 and 32 of the Convention provide a detailed explanation and analysis of the ambiguous expressions of the articles.

So they should follow the principle of honesty and good faith. That means the parties should interpret the meaning of the clause on the premise that it can achieve the reasonable expectations of the other party and on the premise that the object and objective established in the treaty are established. Meanwhile, it should interpret it with legitimate and legitimate purpose, and cannot rely solely on one's own will to arbitrarily interpret the terms.

9.2 Decrease the Burden of Proof in some degree

In specific circumstances, such as when data flows involve legitimate exceptions such as public interests, the law may provide for a simplified standard of evidence , requiring only basic compliance documents (such as data processing agreements, privacy impact assessments, etc.) to be provided, without requiring detailed evidence to be provided one by one. In special circumstances, data controllers are only required to submit a framework agreement or a declaration of compliance without having to provide detailed records of every data transfer or processing.

In some cases, the law can provide for a compliance presumption , that is, it is presumed that their actions comply with relevant regulatory requirements, reducing the complexity of evidence. The burden of proof can be shifted to the data recipient or regulator, requiring them to prove that data protection measures have not been adequately implemented, rather than the data controller bearing the entire burden of proof.

9.3 Limitation of the discretionary rights of the Parties

To understand the term "it considers", the following needs to be considered: first, a description of "the Party" (it). This provision provides for a treaty-making rule in exceptional circumstances. The word "it" in this provision gives the contracting party a sense of autonomy and is entirely up to the contracting party to determine whether the action it takes is in accordance with the exception clause. The word "consider" indicates that the parties have considerable autonomy in determining the substance of the measures they adopt, but it does not imply that the parties have absolute autonomy in the agreement with regard to security. Therefore, "consider" also represents the duty of care on the part of both parties. So it requires the restriction which can be securitized by the third party. The Panels and Appellate Bodies can consider issues that are self-determined by Member States. In the case of the RCEP, although disputes arising from cross-border data flows are completely excluded from the RCEP dispute

settlement mechanism, the RCEP Joint Commission has the power to interpret the provisions, so that in the event of a dispute over the interpretation and application of the basic security interest exception clause, the parties may submit a request for formal explanation to the Joint Commission.

References

[1] Lusine Vardanyan & Hovsep Kocharyan, 'Critical views on the phenomenon of EU digital sovereignty through the prism of global data governance reality: main obstacles and challenges' (2022) 9 (2) European Studies 110.

[2] United Nations Centre on Transnational Corporations, Transnational corporations and transborder data flows; a technical paper (1982)

[3] Branscomb, Anne W, 'Global Governance of Global Networks: A Survey of Transborder Data Flow in Transition.' (1983) 36 Vand. L. Rev. 36 985

[4] Mueller, Milton and Grindal, Karl, 'Is It Trade?' Data Flows and the Digital Economy (Report, August 2018) 1

[5] OECD, Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data, 1980, C (80) 58, Article 1(c)

[6] Mitchell, Andrew D., and Neha Mishra. 'Regulating cross-border data flows in a data-driven world: how WTO Law can contribute.' (2019) Journal of International Economic Law 22 (3) 389

[7] Mitchell, Andrew D., and Neha Mishra. 'Regulating cross-border data flows in a data-driven world: how WTO Law can contribute.' (2019) Journal of International Economic Law 22 (3) 389

[8] Aaronson, Susan Ariel, 'Data is disruptive: How data sovereignty is challenging data governance.' Hinrich Foundation (2021)

[9] U.S. Congress. the Foreign Investment Risk Review Modernization Act of 2018[EB/OL]. (2018-08-13)[2021-11-29]

[10] Donald J. Trump. Continuation of the National Emergency with Respect to Securing the Information and Communications Technology and Services Supply Chain[EB/OL]. (2020-05-14)[2022-11-29]https://www.federalregister.gov/documents/2020/05/14/2020-10594/continuation-of-the-national-emergency-with-respect-to-securing-the-information-and-communications

[11] Stephen Bartholomeusz. Digital trade war: Biden opens new front in effort to contain China[DB/OL](2021-09-01)[2021-10-13]

[12] European Commission. A European Strategy for Data[EB/OL]. (2020-02-19)[2022-12-06]

[13] Article 46. General Data Protection Regulation[Z/OL]. Intersoft Consulting

[14] Homepage(2016-05-04)[2022-12-06]. https://gdpr-info.eu.

[15] European Commission. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)[EB/OL].(2022-06-03)[2022-12-06]

[16] Zheng, Weiwei. "Comparative Study on the Legal Regulation of a Cross-Border Flow of Personal Data and Its Inspiration to China." Frontiers L. China 15 (2020): 280

[17] Calzada, Igor. "Citizens' data privacy in China: The state of the art of the Personal Information Protection Law (PIPL)." Smart Cities 5.3 (2022): 1129-1150

[18] Liu, Junchao. "China's Security Assessment Measures for Outbound Data Transfers." JE Asia & Int'l L. 16 (2023): 267

[19] Russian Data Protection Laws: Essential Guide on Compliance Requirements in Russia, at https://incountry.com, March19, 2021

[20] Savelyev, Alexander. "Russia's new personal data localization regulations: A step forward or a self-imposed sanction?." Computer law & security review 32.1 (2016): 128-145

[21] Medvedev, Sergey. "Data protection in russian federation: overview." Thomson Reuters Practical Law (2016)

[22] Singh, Seema. "Regulation of Cross-Border Data Flow and Its Privacy in the Digital Era." NUJS J. Regul. Stud. 9 (2024): 38

[23] Tan, Johanna G. "A comparative study of the APEC privacy framework-a new voice in the data protection dialogue?." Asian journal of comparative law 3 (2008): 1-44

[24] Mattoo, Aaditya, and Joshua P. Meltzer. "International Data Flows and Privacy." Development Research (2018)

[25] Galagan, Dmytro. "The First Bilateral Investment Treaties: US Postwar Friendship, Commerce, and Navigation Treaties." (2017): 646

[26] Yoo, Ji Yeong, and Dukgeun Ahn. "Security exceptions in the WTO system: bridge or bottle-neck for trade and security?." Journal of International Economic Law 19.2 (2016): 417-444

[27] Desta, Melaku Geboye. "The Law on International Trade in Agricultural Products: From GATT 1947 to the WTO Agreement on Agriculture." (2002): 1-486
[28] Azmi, Ida Madieha Abdul Ghani, and Jeong Chun Phuoc. "INTERNATIONAL NORMS IN REGULATING ECOMMERCE: THE ELECTRONIC COMMERCE CHAPTER OF THE COMPREHENSIVE TRANS-PACIFIC PARTNERSHIP AGREEMENT." International Journal of Business & Society 21 (2020)
[29] Wolfe, Robert. "Learning about digital trade: Privacy and E-commerce in CETA and TPP." World Trade Review 18.S1 (2019): S63-S84
[30] Petros C. Mavroidis, The General Agreement on Tariffs and Trade: A Commentary, Oxford University, 2005
[31] Shukla, Surya Pal. "From GATT to WTO and Beyond." (2000)
[32] Jiang, Chengze. "Research on Applying the WTO Security Exception Clause to the Security Dispute Caused by Cross-border Data Flows." 2021 International Conference on Social Development and Media Communication (SDMC 2021). Atlantis Press, 2022
[33] Chen, Tsai-fang. "To judge the" self-judging" security exception under the GATT 1994-A systematic approach." Asian J. WTO & Int'l Health L & Pol'y 12 (2017): 311
[34] Zhao, Shuo. "The Determination of “Basic Security Interests” in the WTO Security Exception Clause." Studies in Law and Justice 2.4 (2023): 92-100
[35] Barradas, Roberto Zapata. "The TPP, a Horizontal Overview." The Comprehensive and Progressive Trans-Pacific Partnership: The Trans-Pacific Partnership, the Comprehensive and Progressive TPP, their Roots in NAFTA and Beyond (2021): 40
[36] Leblond, Patrick. "Uploading CPTPP and USMCA Provisions to the WTO’s Digital Trade Negotiations Poses Challenges for National Data Regulation.
[37] Yoshinori, A., and Policy Research Institute, Ministry of Finance, Japan. "Data localization measures and international economic law: how do WTO and TPP/CPTPP disciplines apply to these measures." Public Policy Review 16.5 (2021): 1-29
[38] Leblond, Patrick. "Uploading CPTPP and USMCA Provisions to the WTO’s Digital Trade Negotiations Poses Challenges for National Data Regulation."
[39] Burri, Mira. "Digital trade rulemaking in free trade agreements." Research Handbook on Digital Trade. Edward Elgar Publishing, 2023. 9-27
[40] Ciuriak, Dan, and Robert Fay. "The USMCA and Mexico’s prospects under the new North American trade regime." Chapter 2 (2021): 45-66
[41] Del Giovane, Chiara, Janos Ferencz, and Javier López González. "The Nature, Evolution and Potential Implications of Data Localisation Measures." (2023)
[42] Lee, Joo Hyoung, and David Collins. "The Digital Economy Partnership Agreement (DEPA): accession to the digital-only regime." Research Handbook on Digital Trade. Edward Elgar Publishing, 2023. 90-101
[43] Kalin, Roman Pascal. "The Emergence of Digital Trade Regulation." Digital Trade and Data Privacy: Cross-border Flows of Personal Data Between Data Protection and Data Protectionism. Cham: Springer Nature Switzerland, 2024. 67-155
[44] Dayday, Czar Matthew Gerard T. "Cross-border data flows and data regulation under international trade law." Phil. LJ 96 (2023): 33
[45] Chin, Yik-Chan, and Jingwu Zhao. "Governing cross-border data flows: International trade agreements and their limits." Laws 11.4 (2022): 63
[46] Zhai, Dusheng. "RCEP Rules on Cross-Border Data Flows: Asian characteristics and implications for developing countries." Asia Pacific Law Review 33.1 (2025): 24-45
[47] Huang, Gui, and Yin Lei. "The norms on cross-border data flows in the RCEP." Asian Journal of Law and Economics 13.3 (2023): 375-404