# Data Localization Measures and International Economic Law: How Do WTO and TPP/CPTPP Disciplines Apply to These Measures?

ABE Yoshinori

***Professor, Faculty of Law, Gakushuin University***

## Abstract

Remarkable development of the data economy and growing awareness of the importance of data in recent years have driven some countries to strengthen their control over data flow. Measures restricting cross-border data transfer or requiring data to be stored within national borders, such as China's 2017 Cybersecurity Law, are known as data localization measures. This article argues that these data localization measures may constitute a breach of the market access commitment or the national treatment commitment under the General Agreement on Trade in Services (GATS), while there is a fair possibility that these measures are justified under GATS general or security exceptions. It also shows that the E-Commerce Chapter of the Trans-Pacific Partnership / Comprehensive and Progressive Agreement for Trans-Pacific Partnership (TPP/CPTPP) is applicable to cross-border data transfer by companies in non-service sectors as well and contains specific provisions concerning cross-border data transfer and location of computing facilities. This means that the TPP/CPTPP established clearer rules than the GATS with respect to data localization measures. However, as the TPP/CPTPP E-Commerce Chapter has specific exceptions for measures implemented to achieve a legitimate public policy objective, such exceptions could provide broad justification for data localization measures.

Keywords: digital trade, cross-border data transfer, international economic law, WTO, TPP/CPTPP

JEL Classification: F13, K33

## I. Introduction

The data economy has developed remarkably in recent years. Digital platformers, represented by GAFAM, have grown rapidly with vast amounts of data, and in 2020 GAFAM's market capitalization exceeded $5 trillion.[1] Data is the source of wealth in the 21st century, like oil in the 20th century, and has come to be considered as a new "critical resource."[2] Therefore, it can be said that a country that possesses a large amount of data is a "data-rich country" and the global competition for data has begun.

As the importance of such data has been strongly recognized, some countries have be-

[1] CNBC, Amazon, Apple, Facebook and Microsoft close at all-time highs as Big Tech rallies back from coronavirus, June 9, 2020, https://www.cnbc.com/2020/06/09/amazon-apple-facebook-microsoft-close-all-time-high-big-tech-rally.html.

[2] OECD (2019), p. 1.

gun to "enclose" data. A typical example is China, and on June 1, 2017, China enforced its Cybersecurity Law which aims to guarantee the security of the network and requires the operators of "important information infrastructure" to save domestically the personal information and "important data" obtained in China. It also stipulated that the "safety assessment" must be cleared when transferring such data outside China.[3] In this paper, laws and regulations that restrict cross-border transfer of such certain data are referred to as "data localization measures."[4]

There is no universal definition of data localization measures at the moment, but these measures can be broadly divided into two categories. In a narrow sense, data localization measures require enterprises to domestically store data related to their local business activities (domestic storage requirement), or require them to install data processing servers domestically (domestic facility installation requirement).[5] The Chinese Cybersecurity Law can be classified as a data localization measure in a narrow sense.

Broadly defined data localization measures include not only narrow data localization measures but also measures that regulate the cross-border transfer of such data for the purpose of protecting the privacy and personal information of the public.[6] For example, the General Data Protection Regulation (GDPR) of the EU is not a data localization measure in a narrow sense because it does not impose domestic storage or domestic facility installation requirements. Since the GDPR regulates cross-border transfer of data from the perspective of personal information protection, it is a broad data localization measure. Recent academic research on the relationship between data localization and the rules of WTO and FTAs often analyze data localization measures widely.[7] Therefore, this paper also analyzes data localization measures in a broad sense from the point of view of the international economic law disciplines.

In the following sections, the author outlines some typical data localization measures and then discusses the consistency of those measures with the WTO's General Agreement on Trade in Services (GATS) and the Trans-Pacific Partnership Agreement / Comprehensive and Progressive Agreement for Trans-Pacific Partnership (TPP/CPTPP). Through these analyses this paper attempts to clarify the current legal status of data localization measures under international economic law.[8]

---

[3] Asai (2018), pp. 47-48.
[4] Hodson (2018), p. 2.
[5] Ministry of Internal Affairs and Communications (2018), p. 21; Sen refers to data localization measures in a narrow sense as "*de jure* restrictions." See, Sen (2018), p. 325.
[6] Ministry of Internal Affairs and Communications (2017), p. 91; Meltzer (2015), p. 5; Sen calls data localization measures in a broad sense as "*de facto* restrictions." See, Sen (2018), p. 325.
[7] Hodson (2018), p. 2; Chung (2018), pp. 188-192; Crosby (2016), p. 2; Peng and Liu (2017), pp. 192-194.
[8] The data localization measures may be related to international investment agreements, but due to space limitations, we will leave this to another article. In this regard, see, for example, Mitchell and Hepburn (2017), pp. 216-228.

## II. Overview of Data Localization Measures in Major Countries

### *II-1. China*

As mentioned above, China enforced the Cybersecurity Law in 2017 and its Article 37 stipulated data localization regulations as follows:

> Personal information and other important data gathered or produced by critical information infrastructure operators during operations within the mainland territory of the People's Republic of China, shall store it within mainland China. Where due to business requirements it is truly necessary to provide it outside the mainland, they shall follow the measures jointly formulated by the State network information departments and the relevant departments of the State Council to conduct a security assessment; but where laws and administrative regulations provide otherwise, follow those provisions.[9]

Because this provision requires "critical information infrastructure operators" to store personal information and important data within mainland China, it is a data localization measure in a narrow sense. According to Article 31, "critical information infrastructure" denotes "public communication and information services, power, traffic, water, finance, public service, electronic governance and other critical information infrastructure that if destroyed, losing function or leaking data might seriously endanger national security, national welfare and the people's livelihood, or the public interest, on the basis of their tiered protection system." Although Article 31 provides that the State Council will formulate the specific scope of the "critical information infrastructure," the precise meaning of the term is still unclear.

Moreover, though the domestic storage obligations include not only personal information but also "important data," the Chinese Cybersecurity Law does not define the later concept. The draft Measures for Security Assessment of Cross-Border Transfer of Personal Information and Important Data, which are the implementation of the Cybersecurity Law, only provides that "important data" means data closely related to national security, economic development, or social public interests.[10] The draft Guidelines for Cross-Border Data Transfer Security Assessment illustrates examples of "important data" for 27 industrial fields, but it also provides that there remains a possibility of "important data" in other fields.[11]

Regarding the transfer of data outside the mainland of China, the second sentence of Article 37 of the Cybersecurity Law stipulates that the State network information departments

---

[9] In this paper, the English translation of the text of the Chinese Cybersecurity Law is based on "China Law Translate," https://www.chinalawtranslate.com/2016-cybersecurity-law/.

[10] Ministry of Economy, Trade and Industry (2019), Report on Compliance by Major Trading Partners with Trade Agreements: WTO, EPA/FTA and IIA, Addendum 2: Electronic Commerce, pp. 512-513, https://www.meti.go.jp/english/report/data/2019WTO/pdf/02_20.pdf.

[11] *Ibid*.

and the relevant departments of the State Council jointly conduct a security assessment but where laws and administrative regulations provide otherwise, critical information infrastructure operators shall follow those provisions. The draft Measures for Security Assessment of Cross-Border Transfer of Personal Information and Important Data, supplemented by the draft Guidelines for Cross-Border Data Transfer Security Assessment, stipulates some restrictions on cross-border transfer of personal and important data.[12] First, personal information may not be transferred outside the mainland without the consent of the person concerned. Second, if the data to be transferred may affect China's national security or impede public interests, such transfer of the data shall not be allowed. Third, relevant authorities may prohibit the cross-border transfer of data in other cases.[13] Thus, transfer of wide range of personal information and other data may be restricted.

### *II-2. Russia*

On 21 July 2014, the President of the Russian Federation signed Federal Law 242-FZ,[14] which came into force on September 1, 2015. This law amended Federal Law 152-FZ (Personal Information Act) of 2006,[15] introducing data localization regulations.[16] Article 2 of Federal Law 242-FZ added a following new paragraph (Paragraph 5) to Article 18 of Federal Law 152-FZ:

> 5. During personal data collection, inter alia, through the internet, the operator shall ensure that databases located within the Russian Federation are used to record, systematize, accumulate, store, clarify (update or modify) and retrieve personal data of citizens of the Russian Federation, except for cases specified in clauses 2, 3, 4, 8 of part 1 of Article 6 of this Federal Law.

This provision introduces a domestic data storage requirement, making the law a data localization measure in a narrow sense.[17]

In addition, Article 12 (1) of Federal Law 152-FZ states that cross-border transfer of personal data may be allowed when the transfer is carried out into the territory of foreign states which are the parties to the Council of Europe Convention for the Protection of Individuals with Regard to the Processing of Personal Data,[18] as well as other foreign states providing adequate protection of the data subjects' rights. It also stipulates that cross-border

[12] Asai (2018), pp. 47-48.
[13] Asai (2018), p. 78.
[14] See Roskomnadzor 's site for federal law 242-FZ (2014 Personal Information Act Amendment) text, https://pd.rkn.gov.ru/authority/p146/p191/.
[15] See Roskomnadzor 's site for federal law 152-FZ (Personal Information Act 2006) text, https://pd.rkn.gov.ru/authority/p146/p164/.
[16] Mihaylova (2016), pp. 316-317.
[17] Selby (2017), p. 222; KPMG (2018).
[18] Convention for the Protection of Individuals with Regard to the Processing of Personal Data, https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

data transfer may be prohibited or restricted "for the purposes of protecting the foundations of the constitutional order of the Russian Federation, public morality and health, rights and legitimate interests of citizens and providing for national defence and state security."[19] Article 12 (2) provides that the authorized body (Roskomnadzor)[20] makes up a list of foreign states that provides "adequate protection" of personal data under Paragraph 1. The cross-border transfer of personal data into the territories of foreign states that do not provide an adequate protection of the personal data subjects' rights may be carried out, inter alia, where the personal data subject has given his/her consent to the cross-border transfer of his/her personal data, or for the purpose of the performance of a contract to which the personal data subject is a party.[21]

### *II-3. EU*

In the EU, the GDPR has been applied since May 25, 2018. With respect to a cross-border transfer of personal data, Article 44 of the GDPR provides:

> Article 44 General principle for transfers
> Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

Under this rule, the scope of the regulations is limited to the transfers of personal data and there is no concept corresponding to that of "important data" in the Chinese Cybersecurity Law. Furthermore, since the GDPR does not impose a domestic storage requirement or domestic facility installation requirement, it can be categorized as a data localization measure in a broad sense. The transfer of personal data outside the EU will only be allowed if "the conditions laid down in this Chapter are complied with by the controller and processor." The brief overview of the conditions is as follows.

First, if the European Commission makes an "adequacy decision" on a third country in question, transfers of personal data to the third country will be allowed. Article 45 (1) of the GDPR set out the principle of the "adequacy decision":

> Article 45 Transfers on the basis of an adequacy decision

[19] Article 12 (1) of Federal Law 152-FZ, https://pd.rkn.gov.ru/authority/p146/p164.
[20] Article 23 of Federal Law 152-FZ.
[21] Article 12 (4) of Federal Law 152-FZ.

> 1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

The adequacy decision is a finding on whether a third country in question ensures a sufficient protection for personal data, and if the level of the protection by the third country is equivalent to that guaranteed by the GDPR in the EU, the Commission will find the third country provides an adequate level of protection.[22] When assessing the adequacy level of protection, the European Commission shall take into account various factors of the state concerned, including its current legal system and law enforcement on personal data protection, and international arrangements such as treaties in which the third country participates.[23] To date, the EU has found "adequacy" for 12 countries and regions, including Canada and Japan.[24]

Secondly, with respect to a third country that has not been found as ensuring adequate level of protection, cross-border transfers of personal data within a group of companies in accordance with the "Binding Corporate Rules" (BCRs) may be allowed.[25] Article 4 (20) of the GDPR defines the BCRs as follows:

> Article 4 Definition
> (20) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

The BCRs are rules that a corporate group must comply with when transferring personal data from the EU to the outside of the EU within the same group company and that are approved by the "competent supervisory authority" of an EU member state.[26] The BCRs must specify, inter alia, the structure of the corporate group in question, the categories of personal data concerned, the manner of the application of the GDPR principles, the means to exercise the rights of data subjects, and the liability for any breaches of the BCRs.[27]

Thirdly, cross-border transfers of personal data will also be allowed when a data provider within the EU and a data recipient outside the EU conclude a contract containing "Stan-

[22] Mattoo and Meltzer (2018), pp. 775-776.
[23] Article 45(2) of the GDPR.
[24] The European Commission Adequacy Decisions, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.
[25] Article 46 (1) and 2 (b) of the GDPR.
[26] Article 47 (1) of the GDPR.
[27] Article 47 (2) of the GDPR.

dard Date Protection Clauses" (SDPC).[28] However, since the SDPC, to date, has not been adopted by the European Commission,[29] the "Standard Contractual Clauses" (SCC) under the Data Protection Directive 95,[30] which is the predecessor of the GDPR, are still valid[31] and the cross-border transfers of personal data in accordance with the SCC are permitted.[32]

### *II-4. Japan*

In Japan, the provision of personal information to a third party in a foreign country is restricted by Article 24 of the Act on the Protection of Personal Information (APPI) which reads:

> Article 24 (Restriction on Provision to a Third Party in a Foreign Country)
> A personal information handling business operators, except in those cases set forth in each item of the preceding Article, paragraph (1), shall, in case of providing personal data to a third party (excluding a person establishing a system conforming to standards prescribed by rules of the Personal Information Protection Commission as necessary for continuously taking action equivalent to the one that a personal information handling business operator shall take concerning the handling of personal data pursuant to the provisions of this Section; hereinafter the same in this Article) in a foreign country (meaning a country or region located outside the territory of Japan; hereinafter the same) (excluding those prescribed by rules of the Personal Information Protection Commission as a foreign country establishing a personal information protection system recognized to have equivalent standards to that in Japan in regard to the protection of an individual's rights and interests; hereinafter the same in this Article), in advance obtain a principal's consent to the effect that he or she approves the provision to a third party in a foreign country. In this case, the provisions of the preceding Article shall not apply.

This clause, as a general rule, does not permit cross-border transfers of personal data without the consent of the data subject, but there are the following exceptions.

The first exception is for data transfers to a country recognized by the Personal Information Protection Commission (PPC) as "a foreign country establishing a personal information protection system recognized to have equivalent standards to that in Japan in regard to the

---

[28] Article 46(2)(c) of the GDPR.

[29] Scope Europe, *Standard Data Protection Clauses: Explanatory Note to the draft of the SDPC according to Art. 46(1) GDPR*, edition May 2020, p. 4, https://scope-europe.eu/fileadmin/scope/files/SDPC_Explanatory_Note.pdf.

[30] Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] OJ L 281/31, 23.11.1995, p. 31-50.

[31] Standard Contractual Clauses (SCC), https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

[32] Article 46 (5) of the GDPR. In addition, cross-border transfers of personal data with the consent of the data subject (Article 49(1)(a)), with an approved code of conduct (Article 46(2)(e)), or with an approved certification mechanism (Article 46(2)(f)) may be allowed.

protection of an individual's rights and interests." This mechanism is similar to the adequacy decision under the GDPR and currently the 28 EU member states and three EEA member countries that apply the GDPR (Iceland, Norway, and Liechtenstein) are recognized by the PPC as a foreign country with the "equivalent standards that in Japan."[33] The PPC and the European Commission had carried on a dialogue since April 2016 to develop a framework that enables the smooth transfers of personal information between the two economies and, in July 2018, reached a final agreement.[34] Although this dialogue was conducted under a different framework from the EU-Japan Economic Partnership Agreement (EU-Japan EPA), it was thought to complement and expand the benefits gained from the EPA.[35] On January 23, 2019, Japan and the EU have mutually made their "adequacy decisions."[36]

The second exception is for data transfers to a third party in a foreign country "establishing a system conforming to standards prescribed by rules of the Personal Information Protection Commission as necessary for continuously taking action equivalent to the one that a personal information handling business operator shall take concerning the handling of personal data pursuant to the provisions of this Section." The "standards prescribed by rules of the Personal Information Protection Commission" mentioned here are defined in Article 11 bis of the Enforcement Regulations of the Personal Information Protection Law as follows:

> Article 11 (Standards in the system necessary for continuously taking measures equivalent to those which shall be taken by a personal information handlingbusiness operator)
>
> Standards prescribed by rules of the Personal Information Protection Commission under Article 24 of the Act are to be falling under any of each following item.
>
> (i) a personal information handling business operator and a person who receives the provision of personal data have ensured in relation to the handling of personal data by the person who receives the provision the implementation of measures in line with the purport of the provisions under Chapter IV, Section 1 of the Act by an appropriate and reasonable method
>
> (ii) a person who receives the provision of personal data has obtained a recognition based on an international framework concerning the handling of personal infor-

[33] The Public Notice (Kokuji) of the Personal Information Protection Committee, No. 1, 2019, https://www.ppc.go.jp/files/pdf/200201_h31iinkaikokuji01.pdf. The United Kingdom will be treated as a foreign country with the "equivalent standards that in Japan" after Brexit. See, The Public Notice (Kokuji) of the Personal Information Protection Committee, No. 5, 2019, https://www.ppc.go.jp/files/pdf/kokuji_1.pdf.

[34] Joint Press Statement by Haruyo Kumazawa, Member of the Personal Information Protection Commission and Commissioner of the European Commission for Bella Yourober (in charge of justice, consumers and gender equality) (Tokyo, July 17, 2018) https://www.ppc.go.jp/enforcement/cooperation/cooperation/300717/.

[35] Unlike the TPP/CPTPP, there is no provision in the EU-Japan EPA that stipulates the freedom of cross-border data transfer. However, Article 8.81 of the EPA provides that "the two Parties will reassess the need to include provisions in this Agreement for the free circulation of data within three years from the date of its entry into force."

[36] Joint Press Statement by Haruyo Kumazawa, Member of the Personal Information Protection Commission and Commissioner of the European Commission for Bella Yourober (in charge of justice, consumers and gender equality) (January 23, 2019), https://www.ppc.go.jp/files/pdf/310123_pressstatement.pdf. The PPC has established "complementary rules" regarding the handling of personal information transferred from the EU based on adequacy decisions, https://www.ppc.go.jp/files/pdf/Supplementary_Rules.pdf.

mation

Item (i) sets out the case where "appropriate and reasonable" measures are taken between a domestic personal information handling business operator and a foreign third party. The Guidelines on the APPI describe the examples of an "appropriate and rational method": (1) when entrusting the handling of personal data to a business operator in a foreign country, a contract, a confirmation note, and a memorandum between the provider and the receiver (this method is similar to the EU's SDPC or SCC); (2) when transferring personal data within the same corporate group, internal regulations or privacy policies that are commonly applied to the providers and the receivers (this method corresponds to the EU's BCR).[37] Item (ii) prescribes the case where a third party in a foreign country obtained a recognition based on an international framework concerning the handling of personal information, including the APEC's Cross-Border Privacy Rules (CBPR).[38] In addition, when the provision of personal data to a third party without the consent of the person concerned is allowed based on Article 23 of the APPI, cross-border transfers of the same personal data will also be allowed.[39]

### *II-5. Conclusion*

The overview of data localization measures in four countries/regions above reveals that the Chinese Cybersecurity Law is the most restrictive among them because it imposes the domestic data storage obligation and restricts the cross-border transfers of "important data" as well as personal data. It can be said that the scope of the Russian measure is narrower than the Chinese measure since the domestic data storage requirement imposed by Russia concerns personal data only. The measures of the EU and Japan are not restrictive as compared to those of China and Russia, as they do not include a domestic data storage requirement.[40]

## III. Consistency of Data Localization Measures with the GATS

This section examines whether the data localization measures outlined above are consistent with the obligations under the GATS. Firstly, we will look into the applicability of the concept of "measures by Members affecting trade in services" in the GATS to the data localization measures. If a data localization measure can be characterized as a "measure affecting trade in services," GATS's obligations apply to the measure. Secondly, potential conflicts between the GATS's obligations and the data localization measures will be analyzed. It will

[37] Section 4-1 of the Guidelines for the Act on the Protection of Personal Information (Foreign Third Party Edition) (November 2016 (Partially revised in January 2019)), https://www.ppc.go.jp/files/pdf/190123_guidelines02.pdf.
[38] *Ibid*., Section 4-3.
[39] *Ibid*., Section 2.
[40] For an overview of data localization measures in countries other than the four countries/regions examined in this paper, See Mitsubishi UFJ Research & Consulting (2018), pp. 235-247.

reveal that the data localization measures may be inconsistent with Article II (Most-Favored Nation Treatment), Article VI (Domestic Regulation), Article XVI (Market Access), and Article XVII (National Treatment) of the GATS. Finally, we examine whether the inconsistencies of the data localization measures with the GATS obligations can be justified by exception clauses. Although there remain some uncertainties, WTO Members may defend their data localization measures by invoking Article XIV (General Exceptions) or Article XIV bis (Security Exceptions).

## *III-1. Trade in Services under the GATS and Data Localization Measures*

### III-1-1. Four Modes of Cross-Border Service Supply Defined by the GATS

Article I of the GATS stipulates that trade in services is defined as four types of cross-border service supply, and the GATS applies to "measures by Members affecting trade in services." Thus, we will first examine how data localization measures can affect trade in services. Article I(2) of the GATS refers to the four modes of service supply:

> 2. For the purposes of this Agreement, trade in services is defined as the supply of a service:
> (a) from the territory of one Member into the territory of any other Member;
> (b) in the territory of one Member to the service consumer of any other Member;
> (c) by a service supplier of one Member, through commercial presence in the territory of any other Member;
> (d) by a service supplier of one Member, through presence of natural persons of a Member in the territory of any other Member.

Subparagraph (a) corresponds to the case where the service is provided across the border (Mode 1). Its example is the cross-border provision of legal services via the telephone or the internet. Subparagraph (b) sets out "Mode 2" which refers consumption of service abroad. Mode 2 includes lodging or food service supply to overseas travelers. Subparagraph (c) stipulates the cases where service providers establish commercial presence abroad and supply their services to consumers there (Mode 3). Providing financial service through overseas subsidiaries is an example of Mode 3. Subparagraph (d) lays down service supply by movement of service providers who are "natural persons" (Mode 4). In this case a service supplier who is a natural person (e.g. a singer) travels abroad and provides service in that country.

### III-1-2. Mode 1

Of the four, Mode 1 is most relevant to data localization measures. When considering whether a supply of service comes under Mode 1, the principle of "technological neutrality" is applied.[41] According to this principle, any cross-border service supply may be considered as Mode 1 regardless of the means of delivery that are used. For example, various online services, such as distance learning services and video distribution services via the internet,

can meet Mode 1 conditions. Thus, if data localization measures are applied to the personal information or other data collected through these online services, these measures will be considered as "measures affecting trade in services" to which the GATS obligations are applied.

Services under the GATS also include data processing services and database services. The WTO members committed to liberalization of trade in services under the GATS in accordance with the Services Sectoral Classification List ("W/120") which was created in 1991 during the Uruguay Round negotiations, and the W/120 classified "Data processing services" and "Data base services" under the sector of the "Computer and Related Services."[42] The sub-sector of "Data processing service" corresponds to class 843 of the United Nations Provisional Central Production Classification ("CPC") on which the W/120 is based and CPC843 ("Data processing services") covers a wide range of data processing operations.[43] Moreover, the sub-sector of "Data base service" is equivalent to the CPC844 ("Database services") which in turn includes "all services provided from a primarily structured database through a communication network."[44] Thus, "Data processing services" and "Data base services" under the GATS will include cloud services, social network services (SNS), search engine services, etc.[45] This means that if a data localization measure imposes domestic data storage obligations or prohibits foreign data transfers, the provision of data processing services and database services in Mode 1 will be affected, and such a data localization measure could be considered as a "measure that affects trade in services" under the GATS.[46]

In the case of Mode 1 service provision, a data localization measure may be applied extra-territorially, because the service providers are located outside the country that applies the measure. For instance, Article 3.2 (a) of the GDPR stipulates that it applies to the processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU, where the processing activities are related to the offering of goods or services to such data subjects in the EU. Therefore, the regulations of the GDPR will be applied to the provision of data processing services and database services in Mode 1.

### III-1-3. Mode 3

Data localization measures may also affect Mode 3 of service supply (i.e. provision of services through "commercial presence"). For example, when a foreign company establishes its local subsidiary to provide retail services in a host country, and if cross-border data trans-

---

[41] Panel Report, *United States - Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WT/DS285/R, paras. 6.285-6.287.

[42] MTN.GNS/W/120, 10 July 1991, p. 2.

[43] United Nations (1991), p. 238.

[44] *Ibid*.

[45] Crosby (2016), p. 6; Willemyns noted that cloud services are one of the means of service supply rather than service itself and that, for example, email services using cloud technology will be categorized as "electronic mail" (one of the telecommunications services under W/120) instead of data processing services or database services. Willemyns (2019), p. 75.

[46] Hodson (2018), pp. 10-11. Hodson pointed out that WTO Members' commitments on "On-line information and data base retrieval" services may also be relevant in disciplining digital trade barriers. See, Hodson (2018), p. 12. Tuthill and Roy also wrote that the scope of computer related services and that of telecommunications services may overlap with regard to ICT related services. Tuthill and Roy (2012), p. 164.

fer for analyzing its customer data in its home country is restricted, such a restriction will be a measure affecting its Mode 3 service provision. Since data analysis is critically important in service businesses in recent years, data localization measures can widely affect the Mode 3 service supply. Thus, while in the case of Mode 1, only limited service sectors such as online services and data processing services could be affected by data localization measures, in the case of Mode 3, many service sectors may be influenced by data localization measures, taking into account the possibility of the analysis in the home country of data obtained in the host country[47].

## *III-2. GATS Obligations and Data Localization Measures*

As analyzed above, if data localization measures affect trade in services and consequently the GATS applies to these measures, the next question is what obligations under the GATS are relevant to them. In this section, we will discuss Article II (Most-Favored-Nation Treatment), Article VI (Domestic Regulation), Article XVI (Market Access), and Article XVII (National Treatment) sequentially.

### III-2-1. MFN Treatment Obligation

First, one of the obligations that data localization measures may be related to is the MFN treatment obligation. Article II:1 of the GATS sets out:

> Article II: Most-Favoured-Nation Treatment
> 1. With respect to any measure covered by this Agreement, each Member shall accord immediately and unconditionally to services and service suppliers of any other Member treatment no less favourable than that it accords to like services and service suppliers of any other country.

The provision obliges WTO Members to treat any services or service providers indiscriminately irrespective of their origin if they are "like." Also, since the MFN treatment obligation applies to "any measures covered by this Agreement," a member state taking a data localization measure must comply with the obligation regardless of whether or not the member state has made its liberalization commitments in the service sector that is related to the measure in question. Accordingly, if only certain countries' services or service providers are subject to a data localization measure, or if only certain countries' services or service providers are exempted from such a measure, it is likely to constitute a violation of Article II:1.[48] Data transfer regulations based on adequacy decisions, such as those adopted by the EU, Japan, and Russia, may be considered as measures to accord more favorable treatment

[47] In this paper, we examined Mode 1 and Mode 3, but other modes may be relevant to data localization measures. Reyes as well as Mitchell and Hepburn point out that services over the internet may fall under Mode 2. See, Reyes (2011), p. 149 and Mitchell and Hepburn (2017), p. 197.
[48] Mitchell and Hepburn (2017), p. 199.

to the services or the service providers of the countries that are determined as ensuring an "adequacy level of protection" than the services or service providers of the other countries. However, if the services or service providers in question are not "like," different treatments in accordance with adequacy decisions are not inconsistent with the MFN treatment obligation. For example, it can be argued that because cloud services originating from countries affording different levels of personal data protection may not be regarded as "like," data localization measures with adequacy decisions will not be inconsistent with Article II.[49]

Regarding the determination of "likeness" under Article II:1 of the GATS, the Appellate Body in *Argentine - Financial Services* stated that "in principle, a complainant may establish "likeness" by demonstrating that the measure at issue makes a distinction between services and service suppliers based exclusively on origin."[50] This interpretive framework is referred to as the "presumption approach" which is also adopted in the determination of "likeness" of goods under Articles I and III of the GATT. The distinction between a service or service provider in a country that is recognized as providing adequate protection and a service or service provider in a country that is *not* recognized as such would not be the distinction exclusively based on their "origins." Rather it would be the distinction based on the situations of personal information protection in the "origins."

Assuming that the presumption approach is not adopted, the "likeness" test will be applied in order to determine whether services or service providers in question are "like." With respect to trade in goods, the assessment of "likeness" has been based on the following four criteria: products' physical characteristics, products' end uses, consumers' taste and habits, and products' tariff classification.[51] The Appellate Body in *Argentina - Financial Services* stated that to the extent appropriate, the "likeness" test employed in the context of trade in goods may be employed also in assessing "likeness" in the context of trade in services and that the fundamental purpose of the "likeness" test was to assess whether and to what extent the services or service suppliers at issue were in a competitive relationship.[52] According to this analytical framework, if consumers are interested in how a service or service provider protects personal information, such consumers' perceptions of the service or service provider may be taken into account in the "likeness" test. This will lead to a conclusion that the services or service providers originated from countries of different levels of protection of personal information are not "like" and the different treatment based on adequacy decisions does not constitute a breach of the MFN treatment obligation.[53] Furthermore, even if being inconsistent with Article II:1, a data localization measure may be justified under Article XIV (general exceptions) or Article XIV bis (security exceptions). Section 3 below will discuss this possibility.

---

[49] Yakovleva (2018), p. 491.
[50] Appellate Body Report, Argentina - Measures Relating to Trade in Goods and Services, WT/DS453/AB/R, para. 6.38.
[51] Van den Bossche and Zdouc (2017), p. 358.
[52] Appellate Body Report, Argentina - Measures Relating to Trade in Goods and Services, WT/DS453/AB/R, paras. 6.30-6.34.
[53] Yakovleva (2018), p. 491.

### III-2-2. Rational Implementation of Domestic Regulations

Article VI:1 of the GATS stipulates a duty of rational implementation of domestic regulations as follows:

> Article VI: Domestic Regulation
> 1. In sectors where specific commitments are undertaken, each Member shall ensure that all measures of general application affecting trade in services are administered in a reasonable, objective and impartial manner.

The provision requires a WTO Member to implement generally applicable laws, regulations, and procedures relating to trade in services in a reasonable, objective and impartial manner. This obligation, unlike the MFN treatment obligation, applies only in the sectors in which a Member has made its specific commitments, while the application of the obligation would not be affected even if the Member sets out limitations or conditions to its commitments in its Schedule.[54] Thus, a data localization measure generally applicable to all the service sectors would be subject to Article V:1 and required to be implemented reasonably, objectively and impartially.[55] Furthermore, Article VI:4 and 5 refers to substantive obligations regarding qualification/license requirements and technical standards:

> 4. With a view to ensuring that measures relating to qualification requirements and procedures, technical standards and licensing requirements do not constitute unnecessary barriers to trade in services, the Council for Trade in Services shall, through appropriate bodies it may establish, develop any necessary disciplines. Such disciplines shall aim to ensure that such requirements are, inter alia:
> (a) based on objective and transparent criteria, such as competence and the ability to supply the service;
> (b) not more burdensome than necessary to ensure the quality of the service;
> (c) in the case of licensing procedures, not in themselves a restriction on the supply of the service.
>
> 5. (a) In sectors in which a Member has undertaken specific commitments, pending the entry into force of disciplines developed in these sectors pursuant to paragraph 4, the Member shall not apply licensing and qualification requirements and technical standards that nullify or impair such specific commitments in a manner which:
> (i) does not comply with the criteria outlined in subparagraphs 4(a), (b) or (c); and
> (ii) could not reasonably have been expected of that Member at the time the specific commitments in those sectors were made.
> (b) In determining whether a Member is in conformity with the obligation under

[54] Krajewski (2008), p. 169.
[55] Mitchell and Hepburn (2017), pp. 199-200.

> paragraph 5(a), account shall be taken of international standards of relevant international organizations applied by that Member.

Paragraph 4 sets out that ensuring that qualifications/license requirements and technical standards do not become unnecessary obstacles to trade in services, the Council for Trade in Services shall develop necessary disciplines for these requirements and standards and paragraph 5 states that until such disciplines are developed, a Member shall not apply the qualification/license requirements and technical standards in a manner specified in subparagraphs 4(a), (b), and (c). The Council has not yet established any discipline on data localization measures. Therefore, if a data localization measure is not transparent or imposes a greater burden than is necessary to ensure the quality of service, it might be inconsistent with Article VI:5.[56]

### III-2-3. Market Access Obligation

As described above, the provision of the data processing service and the database service in Mode 1 will be significantly affected if a WTO Member restricts cross-border transfer of data such as personal information. Such a restriction may be in conflict with GATS Article XVI which sets out market access obligations, because it may limit the access by foreign service suppliers to the markets of the Member at issue. Article XVI:2 (a) and (c) provides as follows:

> 2. In sectors where market-access commitments are undertaken, the measures which a Member shall not maintain or adopt either on the basis of a regional subdivision or on the basis of its entire territory, unless otherwise specified in its Schedule, are defined as:
> (a) limitations on the number of service suppliers whether in the form of numerical quotas, monopolies, exclusive service suppliers or the requirements of an economic needs test;
> (c) limitations on the total number of service operations or on the total quantity of service output expressed in terms of designated numerical units in the form of quotas or the requirement of an economic needs test;

The Appellate Body in *US - Gambling* found that the United States' ban on the cross-border supply of online gambling and betting services was "zero quota," violating paragraphs (a) and (c) of Article XVI:2.[57] Some authors indicated that, following the Appellate Body's finding in *US - Gambling*, a measure limiting the cross-border transfer of data may be regarded as a limitation of the number of providers of online data processing / database services or a limitation of the total number of such businesses.[58] Having said that, be-

[56] *Ibid.*
[57] Appellate Body Report, *United States - Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WT/DS285/AB/R, paras. 238, 251.

cause the market access obligations only apply to the service sectors to which a Member made its commitments and are subject to the terms and conditions specified in its Schedule, what is important is the content of the specific commitments made by the Member. For example, China had scheduled its market access commitments for data processing services (CPC843) in Mode 1 without any conditions while making no commitment for database services (CPC848).[59] Thus, whether China's market access obligations apply to its data localization measures will depend on whether the specific services targeted by Chinese measures (for example, cloud services and SNS services) are classified as data processing services or database services.[60]

### III-2-4. National Treatment Obligation

Data localization measures could also be in breach of the national treatment obligation under Article XVII:1 which provides:

> Article XVII: National treatment
> 1. In the sectors inscribed in its Schedule, and subject to any conditions and qualifications set out therein, each Member shall accord to services and service suppliers of any other Member, in respect of all measures affecting the supply of services, treatment no less favourable than that it accords to its own like services and service suppliers.

This provision states in essence that any foreign services or service providers may not be treated less favorably than domestic "like" services or service providers. Having said that, similar to the market access obligation of Article XVI, the national treatment obligation applies only to the service sectors where a Member made its specific commitment, subject to the limitations and conditions described in its Schedule. Thus, the relationship between data localization measures and national treatment obligations will depend on the content of the Schedule of the Member taking the measures. Data localization measures may impose an additional burden on foreign service providers, because the domestic storage requirement or the domestic facility installation requirement could increase their costs.[61] Considering the purpose of Article XVI is to secure equal competitive conditions, de facto discrimination against foreign services or service providers may also be less favorable treatment under this clause.[62] Domestic storage requirements or domestic facility installation requirements on foreign service providers who provide their services in Mode 3, will cast an additional burden on them. Such a treatment would modify the conditions of competition in favor of domestic services or service providers, resulting to violate Article XVII.[63] The EU stated in the

[58] Matto and Meltzer (2018), p. 780; Mitchell and Hepburn (2017), pp. 200-201; Chung (2018), pp. 196-197.
[59] GATS/SC/135, p. 10.
[60] Chung (2018), p. 197.
[61] Crosby (2016), p. 8.
[62] Panel Report, *China - Certain Measures Affecting Electronic Payment Services*, WT/DS413/R, para. 7.700.

Council for Trade in Services that "foreign companies operating in China could find themselves in de facto less competitive situation compared to domestic operators" because of the Chinese cybersecurity law.[64] This statement seems to be based on the EU's perception that the Chinese law will likely breach the national treatment obligations.

## *III-3. GATS Exceptions and Data Localization Measures*

While data localization measures may violate GATS obligations as discussed above,[65] such violations could be justified under Article XIV (general exceptions) or Article XIV bis (security exceptions). This section examines the relationship between data localization measures and these exception clauses.

### III-3-1. GATS Article 14 (General Exceptions)

Article XIV of the GATS, like Article XX of the GATT, provides for the general exceptions which allow WTO Members to take any measure that satisfies the requirements set out in its subparagraphs and chapeau, even if the measure at issue is found as inconsistent with GATS obligations. Article XIV contemplates an analysis in two stages: (i) a panel must determine whether the measure falls within the scope of one of the subparagraphs of Article XIV; and (ii) after having found that the measure at issue is provisionally justified under one of the subparagraphs, the panel must examine whether this measure satisfies the requirements laid down in the chapeau (a "two-tier analysis").[66] The chapeau and subparagraphs of Article XIV that is likely to be relevant to data localization measures are as follows:

> Article XIV: General Exceptions
> Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures:
> (a) necessary to protect public morals or to maintain public order;
> (c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to:

---

[63] Chung (2018), p. 197; Hodson (2018), p. 14. Hodson, mentioning that footnote 10 to Article XVII:1 provides that "[s]pecific commitments assumed under this Article shall not be construed to require any Member to compensate for any inherent competitive disadvantages which result from the foreign character of the relevant services or service suppliers," indicates that it may be more costly for foreign suppliers to meet a data localization requirement by virtue of their foreign character. However, given the current global telecommunications network, it seems to be difficult to conclude that foreign suppliers have "inherent competitive disadvantages" with regard to data localization measures.

[64] Report of the Meeting held on 7 December 2018, S/C/M/137, para. 7.25.

[65] In addition to the provisions discussed in III-2, Crosby argues that Paragraph 5 (c) of Annex on Telecommunications of the GATS requires WTO Members not to restrict cross-border data transfers in the service sectors where they undertake specific commitments. See, Crosby (2016), p. 7.

[66] Appellate Body Report, *US – Gambling*, para. 292.

(i) the prevention of deceptive and fraudulent practices or to deal with the effects of a default on services contracts;
(ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;
(iii) safety.

One of the possible justifications of data localization measures under Article XIV would be the protection of privacy and of confidentiality of individual records. Since subparagraph (c)(ii) sets out "the protection of the privacy of individuals in relation to the processing and dissemination of personal data," data localization measures necessary to ensure compliance with laws related to personal information protection may be fall within this provision.[67] The point here is whether a data localization measure at issue is "necessary" to secure compliance with a personal information protection law or regulation. This test is called as the necessity requirement, and whether or not the requirement is satisfied is determined by "weighing and balancing" a series of factors, including the importance of the value protected by that the measure in question is intended to protect, the contribution of the measure to the objective pursued, and the level of trade-restrictiveness of the measures.[68] Moreover, if a WTO-consistent or less WTO-inconsistent alternative measure is reasonably available, the measure at issue would not be considered as "necessary."[69] Data localization measures that impose domestic data storage obligations, when overly restrictive, could have a large negative impact on trade in services. Such measures may not be provisionally justified by subparagraph (c)(ii) if less trade-restrictive alternative measures are reasonably available.[70]

It is also pointed out that data localization measures may fall within the scope of subparagraph (a).[71] The concept of "public moral" has been interpreted by panels as "standards of right and wrong conduct maintained by or on behalf of a community or nation."[72] Member States have wide discretion in determining what constitutes "public morals." Thus, in a WTO Member, where protection of personal information and privacy is considered to be a fundamentally important right, it could be argued that data localization measures are measures to realize the public moral that personal information and privacy should be protected.[73] However, as with sub-paragraph (c)(ii), the "necessity" requirement must also be satisfied for provisional justification under subparagraph (a).[74]

---

[67] Hodson (2018), p. 16.
[68] Appellate Body Report, *United States - Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WT/DS285/AB/R, para. 306.
[69] *Ibid*., para. 307.
[70] Hodson (2018), p. 17.
[71] *Ibid*., p. 15; Mitchell and Hepburn (2017), p. 202.
[72] Panel Report, *United States - Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WT/DS285/R, para. 6.465.
[73] Mattoo and Meltzer (2018), p. 781.
[74] Mattoo and Meltzer point out that more flexible alternatives could be reasonably available with respect to the GDPR. Mattoo and Meltzer (2018), p. 781-782.

Even if the data localization measures are provisionally justified under subparagraphs (a) or (c)(ii) , as a second step, they cannot be finally justified unless they also meet the requirements of the chapeau. The feature of these requirements is to focus on a "manner of application" of the measure in question.[75] In terms of data localization, how the laws and regulations concerned are actually implemented would be examined. Therefore, if data localization measures are applied inconsistently on a case-by-case basis, a panel would find that these measures have been applied in such a manner which would constitute "a means of arbitrary or unjustifiable discrimination" or "a disguised restriction on trade in services."[76]

### III-3-2. GATS Article XIV bis (Security Exceptions)

With respect to the general exceptions provided in Article XIV of the GATS, we have analyzed the possibility of justifying data localization measures for the purpose of protecting personal information. However, if a WTO Member, like China, adopts a data localization measure with the extended scope of "data" which includes not only personal information but also broadly defined "important data," it would be difficult to justify such a measure on grounds of the protection of privacy or public morals referred to in Article XIV. In this regard, the security exceptions set forth in Article XIV bis might provide a justification for a data localization measure with a wide scope. Article XIV bis:1 stipulates as follows:

> Article XIV bis: Security Exceptions
> 1. Nothing in this Agreement shall be construed:
> (a) to require any Member to furnish any information, the disclosure of which it considers contrary to its essential security interests; or
> (b) to prevent any Member from taking any action which it considers necessary for the protection of its essential security interests:
> (i) relating to the supply of services as carried out directly or indirectly for the purpose of provisioning a military establishment;
> (ii) relating to fissionable and fusionable materials or the materials from which they are derived;
> (iii) taken in time of war or other emergency in international relations; or
> (c) to prevent any Member from taking any action in pursuance of its obligations under the United Nations Charter for the maintenance of international peace and security.

It has been pointed out that measures restricting the cross-border transfer of military information would be justified under subparagraph (a) and measures countering cyber attacks would fall within the scope of subparagraph (b)(iii).[77] An important difference from the general exception clauses is that the text of the security exception clauses contain a so-called

[75] Appellate Body Report, *United States - Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WT/DS285/AB/R, para. 339.
[76] Mitchell and Hepburn (2017), p. 204-205.

"self-judging" element. In terms of subparagraph (a), the phrase "the disclosure of which it considers contrary to its essential security interests" might be interpreted to mean that a Member invoking the defense could determine whether the disclosure of information at issue would be "contrary to its essential security interests" on its own decision. Subparagraph (b) also includes the phrase "which it considers necessary for the protection of its essential security interests," which might imply that an invoking Member may "self-judge" the necessity of the measures.

Article XXI of the GATT also has a "self-judging" character, but the panel *in Russia - Traffic in Transit*, declaring that it had jurisdiction over the security exceptions, found that the discretion of an invoking Member under Article XXI was limited by the obligation of good faith.[78] While this gives a broad discretion for a Member States that invokes the security exceptions, a completely self-judging character of Article XXI was denied. In addition, the panel stated that the adjective clause "which it considers" does not qualifies the subparagraphs of Article XXI of the GATT and that panels would examine objectively whether the requirements of the subparagraphs were met.[79] Therefore, if the same interpretative framework applies to GATS Article XIV bis, WTO panels will objectively determine whether the data localization measures at issue fall within the scope of subparagraphs (b)(i) to (iii).

Note that the United States argued that because GATT Article XXI was self-judging, WTO panels lacked the authority to review the invocation of Article XXI and consequently the dispute was "non-justiciable."[80] It strongly criticized the interpretation of Article XXI adopted by the panel in *Russia - Traffic in Transit*.[81] Because China's Cybersecurity Law covers a wide range of unlimited "important data," if a panel reviews the law based on the principle of good faith, it would be difficult to justify it under GATS Article XIV bis. However, if we take the same position as the United States, the Chinese Cybersecurity Law could be defended by simply invoking the security exception. Having said that, China took a position contrary to that of the United States in interpreting Article XXI of the GATT in *Russia - Traffic in Transit*,[82] it is unlikely that China would defend its data localization measures by arguing that Article XIV bis is "self-judging." On the contrary, for the United States, it could not challenge the Chinese Cybersecurity Law, assuming its own position regarding the security exception clauses. In this way, a somewhat tricky legal situation has arisen regarding the relationship between data localization measures and Article XIV bis.

## IV. TPP /CPTPP Disciplines on Data Localization Measures

So far, we have examined how GATS obligations apply to data localization measures, but the GATS covers only the matters concerning trade in services and there are no rules in

[77] Mitchell and Hepburn (2017), pp. 205-206.
[78] Panel Report, *Russia-Measures Concerning Traffic in Transit*, WT/DS512/R, paras. 7.131-7.133, 7.138-7.139.
[79] *Ibid*., para. 7.101.
[80] *Ibid*., para. 7.52.
[81] Minutes of Meeting of the Dispute Settlement Body, April 26, 2019, WT/DSB/M/428, para. 8.11.
[82] Panel Report, *Russia-Measures Concerning Traffic in Transi*t, WT/DS512/R, para. 7.41.

the GATS that specifically address data localization measures themselves. In that sense, GATS disciplines are behind the rapid progress of data society, which has led to some developments in making specific rules on data localization in FTAs. In the following sections, we will focus on the relevant provisions of the TPP/CPTPP, which are considered to be one of the most advanced disciplines on data localization measures at this stage.

### *IV-1. Cross-Border Data Transfer*

The TPP/CPTPP has a chapter for electronic commerce (Chapter 14), separate from the rules for trade in goods and services. Article 14.11 set forth rules on cross-border data transfer as follows:

> Article 14.11: Cross-Border Transfer of Information by Electronic Means
> 1. The Parties recognise that each Party may have its own regulatory requirements concerning the transfer of information by electronic means.
> 2. Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person.

This provision recognizes the right of the parties to regulate cross-border data transfer in paragraph 1 and imposes on the parties to allow cross-border data transfer for the conduct of the business of "a covered person" in paragraph 2. The concept of " a covered person" is defined in Article 14.1:

> covered person means:
> (a) a covered investment as defined in Article 9.1 (Definitions);
> (b) an investor of a Party as defined in Article 9.1 (Definitions), but does not include an investor in a financial institution; or
> (c) a service supplier of a Party as defined in Article 10.1 (Definitions), but does not include a "financial institution" or a "cross-border financial service supplier of a Party" as defined in Article 11.1 (Definitions);

As described above, "a covered person" means "a covered investment," "an investor of a Party," or "a service supplier of a Party." The concept of "a covered investment" and "an investor of a Party" defined in Article 9.1 will include companies not only in service sectors but also in manufacturing industries. Accordingly, unlike the GATS disciplines, Article 14.11 applies to measures related to cross-border data transfer in the manufacturing industries as well.[83] Subparagraph (b) of Article 14.1 excludes "an investor in a financial institution" from "an investor" and Article 14.1 provides that "a covered person" does not include

[83] Tsuda (2018), p. 12.

"a financial institution" or a "cross-border financial service supplier of a Party." This is because, in the TPP negotiations, the United States requested the exclusion of financial institutions from "a covered person" in order to ensure the effectiveness of prudential regulations.[84]

Article 14.11.2 is notable because it explicitly deals with cross-border data transfer. However, while this provision imposes an obligation to "allow the cross-border transfer of information by electronic means, including personal information," it remains unclear whether states parties can impose conditions on their permissions for the transfer.[85] This raises the following questions. Will Article 14.11.2 be violated only if all data processing is required to be done domestically and no cross-border data transfer is allowed? Or is it also a violation of Article 14.11.2 that state parties require a part of data processing to be carried out within their territories when they allow cross-border data transfer? At this point both interpretations seems to be possible.[86] In addition, Article 14.11.2 stipulates that "Each Party shall allow the cross-border transfers of information," and it does not specify which countries are concerned with "the cross-border transfers of information." Thus, it has been pointed out that there is a possibility that the obligation under Article 14.11.2 will be relevant not only when data transfers are made directly between TPP/CPTPP state parties, but also when data transfers are made between a TPP/CPTPP party and a third country.[87] Accordingly, even when data transfer between two TPP/CPTPP parties takes place via China, a non-TPP country, a regulation on such cross-border data transfer might be an issue under Article 14.11.2.

The TPP/CPTPP also includes an exception to the above-mentioned obligation to permit cross-border data transfer, which allows certain measures for achieving legitimate public policy objectives. Article 14.11.3 provides as follows:

> 3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:
> (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and
> (b) does not impose restrictions on transfers of information greater than are required to achieve the objective.

Under this clause, a measure restricting cross-border data transfer will be justified if it satisfies the following three requirements: (1) the measure is "to achieve a legitimate public policy objective," (2) it is not applied in a manner of arbitrary and unjustifiable discrimination or a disguised trade restriction, and (3) it does not restrict the data transfer more than necessary. Of these, the second and the third requirement are considered to respectively correspond to the requirement of the chapeau and the necessity requirement of GATS Article

[84] Hodson (2018), p. 23.
[85] Tsuda (2018), p. 14.
[86] Chung (2018), p. 200.
[87] Tsuda (2018), pp. 14-15.

XIV. On the other hand, with regard to the first requirement, it seems that the general concept of "a legitimate public policy objective" is broader than the specific exceptions provided under subparagraphs of Article XIV.[88] Thus, what will be justified under this provision when actually applied is unclear at this stage.[89]

### *IV-2. Prohibition of Domestic Facility Installation Requirement*

The requirement of domestic facility installation, one of the data localization measures, is explicitly prohibited by the TPP/CPTPP. Article 14.13 provides:

> Article 14.13: Location of Computing Facilities
> 1. The Parties recognise that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications.
> 2. No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.

Article 14.13.1 recognizes that the TPP/CPTPP parties have the right to impose "its own regulatory requirements regarding the use of computing facilities," but "regulatory requirements" seems to be not related to the requirements of domestic facility installation because this clause states that "requirements that seek to ensure the security and confidentiality of communications" are examples of the "regulatory requirements." Rather, Article 14.13.2 clearly prohibits the requirement of the domestic installation of computer facilities. It should be noted that this clause also obliges the TPP/CPTPP parties not to impose the requirements of use of domestic computer facilities.

In addition, as in Article 14.11, Article 14.13.2 stipulates that "a covered person" shall not be required to use or locate computer facilities domestically. Since the concept of "a covered person" is broader than that of "a service provider," the scope of the application of this clause is wider than that of the relevant GATS provisions. Furthermore, prohibiting domestic facility use and installation requirements regardless of whether such requirements constitute any discrimination between domestic and foreign entities, it can be said that Article 14.13.2 is a stricter discipline on data localization measures than the national treatment provision of GATS Article XVII. This is because, while as mentioned above, under GATS Article XVII, requiring uniformly domestic facility use or installation will be allowed unless it gives disadvantageous treatment to foreign service providers, under TPP/CPTPP Article 14.13.2 the existence of such discriminatory treatment will not be taken into account.

Article 14.13, like Article 14.11, contains an exception for achieving legitimate public policy objectives. Article 14.13.3 provides as follows:

---

[88] Peng and Liu (2017), p. 196.
[89] Chung (2018), p. 200.

> 3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:
> (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and
> (b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective.

This clause employs almost the same wording as Article 14.11.3, and consequently the scope of this exception will depend on what the "legitimate public policy objective" actually means.[90]

## *IV-3. Exception Clauses*

In addition to Article 14.11.3 and Article 14.13.3 which are the specific exceptions to the rules on data localization measures, there are several exception clauses that can be applied to data localization measures in Chapter 29. We will explore these exceptions in this section.

### IV-3-1. General Exceptions

Article 29.1.3 which concerns general exceptions provides as follows:

> 3. For the purposes of Chapter 10 (Cross-Border Trade in Services), Chapter 12 (Temporary Entry for Business Persons), Chapter 13 (Telecommunications), Chapter 14 (Electronic Commerce) and Chapter 17 (State-Owned Enterprises and Designated Monopolies), paragraphs (a), (b) and (c) of Article XIV of GATS are incorporated into and made part of this Agreement, *mutatis mutandis*. The Parties understand that the measures referred to in Article XIV(b) of GATS include environmental measures necessary to protect human, animal or plant life or health.

According to this provision, subparagraphs (a) and (c) of GATS Article XIV applies, *mutatis mutandis*, to Chapter 14 of the TPP/CPTPP. Since subparagraph (a) stipulates the protection of public morals as a justification and subparagraph (c) provides the protection of privacy and personal data as a defense, the above analysis on GATS Article XIV will similarly apply to Chapter 29 of the TPP/CPTPP. The exceptions concerning "a legitimate public policy objective" provided in Article 14.11.3 and Article 14.13.3 can be interpreted to have a broader scope than the justifications specified in subparagraphs (a) and (c) of GATS Article XIV.[91]

[90] Mitchell and Hepburn (2017), p. 211.
[91] Hodson (2018), p. 24.

### IV-3-2. Security Exception Clause

Article 29.2 of the TPP/CPTPP which sets out security exceptions reads as follows:

> Nothing in this Agreement shall be construed to:
> (a) require a Party to furnish or allow access to any information the disclosure of which it determines to be contrary to its essential security interests; or
> (b) preclude a Party from applying measures that it considers necessary for the fulfilment of its obligations with respect to the maintenance or restoration of international peace or security, or the protection of its own essential security interests.

The terms used in subparagraph (a) of this provision are almost the same as those used in subparagraph (a) of GATS XIV bis:1, though the former employs the phrase "it determines" while the later includes the phrase "it considers." Although subparagraph (b) of Article 29.2 resembles subparagraphs (b) and (c) of GATS Article XIV bis:1, it simply stipulates a justification for "the protection of its own essential security interests" and does not elaborate what actually constitutes the "essential security interests" of the TPP/CPTPP parties, contrary to subparagraph(b)(i) through (iii) of GATS Article XIV bis:1 which definitively specified the measures that comprise the measures for the protection of the "essential security interests" of the WTO Members. Thus, under TPP/CPTPP Article 29.2, a broad range of security-related measures could be excused, comparing under GATS Article XIV bis. Furthermore, considering both subparagraphs (a) and (b) both contain the self-judging phrases ("it determines" and "it considers" respectively), it could be argued that the discretion of the TPP/CPTPP Parties under this clause is very wide.[92]

## V. Conclusion

As discussed above, under the GATS, there are no provisions that directly stipulate data localization measures. Basically, data localization measures concerning service sectors are subject to the market access and national treatment obligations based on the specific commitments made by each WTO member, but it should be noted that there is much room for justifying these measures by the general exception or security exception clauses. On the other hand, the TPP/CPTPP's e-commerce chapter is applicable to cross-border data transfer by companies not limited to service sectors, so that a wider range of data localization measures will be subject to the discipline of the TPP/CPTPP than the GATS. In addition, because the TPP's e-commerce chapter has explicit provisions regarding the cross-border data transfer and the domestic facility installation requirements, it includes clearer disciplines than those of the GATS regarding data localization measures. However, the TPP/CPTPP seems to leave certain room for defending data localization measures, since there are not only the exception clauses regarding measures to achieve "a legitimate purpose of public policy" in the e-com-

[92] *Ibid*., p. 26.

merce chapter but also the general exception and security exception clauses in Chapter 29 similar to those of the GATS.

It may be argued that the TPP/CPTPP data localization-related provisions are drafted ambiguously on purpose, in order to obtain the agreement of the negotiating countries. Some commentators expect that such a "constructive ambiguity" created by the drafters will be clarified through the dispute settlement when the consistency with the TPP/CPTPP disciplines of the data localization measures is actually disputed.[93] On the other hand, it has been pointed out that how the data localization measures, which involves highly technical issues related to data transfer and data security, should be evaluated under the relevant provisions of the GATS and the TPP/CPTPP will be beyond the capabilities of the judicial bodies such as the WTO panels, the Appellate Body and the TPP/CPTPP panels.[94] In the recent debates over the Appellate Body, its attitude towards the interpretation of the text of the WTO Agreements with "constructive ambiguity" is criticized as "judicial activism," though the debate does not concern data localization measures. Similar issues may arise with the TPP/CPTPP's provisions related to data localization, and it may not be appropriate that the TPP/CPTPP's panels' attempt to resolve problems that the drafters could not.

In this respect, it seems important to activate discussions and work at various councils and committees, which are the administrative mechanisms governing the implementation of the WTO or TPP/CPTPP agreements, rather than the judicial bodies of their dispute resolution mechanisms. Regarding the Chinese Cybersecurity Law, for example, at the Council of Trade in Services tasked with facilitating the operation of the GATS, the United States, Japan, the EU, New Zealand, and Canada posed questions on the content of the law and expressed concern over its consistency with the GATS rules.[95] This process will require China to be accountable on its Cybersecurity Law and will exert peer pressure to operate the law according to the disciplines of the GATS. In the TPP/CPTPP as well, it is conceivable that the operation and interpretation of data localization-related provisions will be clarified under the TPP Commission established by Article 27.1. One of the functions of the Commission is to consider "any matter relating to the implementation and operation of the TPP/CPTPP Agreement" (Article 27.2.1 (a)). The Commission may "develop arrangements for implementing this Agreement" (Article 27.2.2(d)) and "issue interpretations of the provisions of this Agreement" (Article 27.2.2(f)). As the Committee may also establish "any ad hoc or standing committee, working group, or any other subsidiary body" (Article 27.2.2(a)), it may establish an auxiliary body that deals with data localization issues.

It should also be noted that it would be difficult to timely address the problems related to the data economy, which is highly technical and making progress rapidly, only with "hard law" including the WTO and TPP/CPTPP Agreements. We may expect "soft law" to play a role in supplementing such a limit of the hard law. For example, Principle 69 of the 2015 APEC Privacy Framework provides that its member state should refrain from restricting

[93] Peng and Liu (2017), p. 196.
[94] Mitchell and Hepburn (2017), p. 210.
[95] Report of the Meeting held on 7 December 2018, S/C/M/137.

cross-border transfer of personal information between itself and another state where the other state has laws and regulations to implement the Framework or sufficient safeguards, such as the APEC CBPR (Cross Border Privacy Rules), are put in place by their personal information controller.[96] This principle is a kind of soft law that, while raising the protection of personal information to a sufficient level among multiple countries, liberalizes cross-border transfer of personal information among those countries. It can be said that such a "soft law" approach will be another way for tackling the problem of data localization measures regarding personal information. Currently, WTO Members participating in the negotiation of rules on electronic commerce are trying to draft a consolidated text,[97] and the formulation of rules related to data localization is also being considered.[98] It may be necessary that the "hard law" approach including setting out a new WTO agreement on e-commerce and the "soft law" approach for international data flow should complement each other.

## References

Asai, T. (2018) Chinese Cyber Security Act (Internet Security Act), UniServ Publishing (In Japanese).

Bauer, M., H. Lee-Makiyama, E. van der Marel, and B. Verschelde (2015), *Data Localisation in Russia: A Self-imposed Sanction*, https://ecipe.org/wp-content/uploads/2015/06/Policy-Brief-062015_Fixed.pdf.

Chung, C. (2018), "Data Localization: The Causes, Evolving International Regimes and Korean Practices", *Journal of World Trade*, Vol. 52, No. 2, pp. 187-208.

Crosby, D. (2016), *Analysis of Data Localization Measures Under WTO Services Trade Rules and Commitments, E15 Initiative. Geneva: International Centre for Trade and Sustainable Development (ICTSD) and World Economic Forum*, www.e15initiative.org/.

Hodson, S. (2018), "Applying WTO and FTA Disciplines to Data Localization Measures," *World Trade Review*, First View, https://doi.org/10.1017/S1474745618000277.

KPMG, *The "localisation" of Russian citizens' personal data: Compliance with the Russian law on personal data*, https://home.kpmg/be/en/home/insights/2018/09/the-localisation-of-russian-citizens-personal-data.html.

Krajewski, M. (2008), "Article VI GATS", in Wolfrum, R. et al (eds), *WTO - Trade in Services,* Martinus Nijhoss.

Kuan Hon, W. (2017), *Data Localization Laws and Policy: The EU Date Protection Inter-*

[96] APEC Privacy Framework (2015), https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015). See also, Watanabe (2017), p. 199.

[97] WTO News, 23 October 2020, "Negotiations on e-commerce continue, eyeing a consolidated text by the end of the year," https://www.wto.org/english/news_e/news20_e/ecom_26oct20_e.htm.

[98] The EU published its proposal for e-commerce rules on May 3, 2019. While emphasizing the need for cross-border data transfer regulations to ensure the protection of personal data and privacy, it proposed a rule that cross-border data flows shall not be restricted by data localization measures. EU Proposal for WTO Disciplines and Commitments Relating to Electric Commerce, INF/ECOM/22, http://trade.ec.europa.eu/doclib/docs/2019/may/tradoc_157880.pdf.

*national Transfers Restriction Through a Cloud Computing Lens*, Elger.

Li, J.H. (2019) Explanation of the Main Points of "Chinese Cybersecurity Law" (2), https://gvalaw.jp/7509 (In Japanese).

Mattoo, A. and J. Meltzer (2018), "International Data Flows and Privacy: The Conflict and Its Resolution," *Journal of International Economic Law*, Vol. 21, pp. 769-789.

Meltzer, J.P. (2015), "A New Digital Trade Agenda," *E15 Initiative. Geneva: International Centre for Trade and Sustainable Development (ICTSD) and World Economic Forum*, www.e15initiative.org/.

Mihaylova, I. (2016), "Could the Recently Enacted Data Localization Requirements in Russia Backfire?", *Journal of World Trade*, Vol. 50, No. 2, pp. 313-334.

Ministry of Economy, Trade and Industry (2019), Report on Compliance by Major Trading Partners with Trade Agreements: WTO, EPA/FTA and IIA, Addendum 2: Electronic Commerce, pp. 512-513, https://www.meti.go.jp/english/report/data/2019WTO/pdf/02_20.pdf.

Ministry of Internal Affairs and Communications (2017) White Paper 2017 on Information and Communication, http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/pdf/index.html (In Japanese).

Ministry of Internal Affairs and Communications (2018) White Paper 2018 on Information and Communication, http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/pdf/index.html (In Japanese).

Mitchell, A. and J. Hepburn (2017), "Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer," *Yale Journal of Law and Technology*, Vol. 19, pp. 182-237.

Mitsubishi UFJ Research & Consulting (2018) International Economic Research Project (Survey on Regulations Related to Digital Trade) Survey Report on Building Economic Growth Strategies in Japan and Overseas in 2017, https://www.meti.go.jp/meti_lib/report/H29FY/000892.pdf (In Japanese).

OECD (2019), Data in the Digital Age, https://www.oecd.org/going-digital/data-in-the-digital-age.pdf.

Peng, S. and Liu, H. (2017), "The Legality of Data Residency Requirements: How Can the Trans-Pacific Partnership Help?", *Journal of World Trade*, Vol. 51 No. 2, pp. 183-204.

Reyes, C.L. (2011), "WTO-Compliant Protection of Fundamental Rights: Lessons from the EU Privacy Directive," *Melbourne Journal of International Law*, Vol. 12, pp. 141-176.

Sen, N. (2018), "Understanding the Role of the WTO in International Date Flows: Taking the Liberalization or the Regulatory Autonomy Path?", *Journal of International Economic Law*, Vol. 21, pp. 323-348.

Selby, J. (2017), "Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?", *International Journal of Law and Information Technology*, Vol. 25, pp. 213-232.

Tsuda, H. (2018) E-Commerce Chapter in Japan's Economic Partnership Agreements: A Case of the TPP Agreement, http://www.jlea.jp/2018zy_zr/ZR18-08.pdf (In Japanese).

Tuthill, L. and M. Roy (2012), "GATS Classification Issues for Information and Communication Technology Services," in M. Burri and T. Cottier (eds.), *Trade Governance in the Digital Age*, Cambridge University Press.

United Nations (1991), Provisional Central Product Classification, Statistical Papers Series M, No. 77, https://www.wto.org/english/tratop_e/serv_e/cpc_provisional_complete_e.pdf.

Watanabe, S. (2017), "Regulating Barriers for Cross-Border Personal Data Transfers: Searching for Roles of International Economic Law," *International Economic Law,* No. 26, pp. 188-212 (In Japanese).

Willemyns, I. (2019), "GATS Classification of Digital Services - Does 'The Cloud' Have a Silver Lining?", *Journal of World Trade*, Vol. 53, No. 1, pp. 59-82.

Yakovleva, S. (2018), "Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?", *World Trade Review*, Vol. 17, No. 3, pp. 477-508.

## Related WTO cases

Panel Report, *United States - Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WT/DS285/R, adopted 20 April 2005.

Appellate Body Report, *United States - Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WT/DS285/AB/R, adopted 20 April 2005.

Panel Report, *China - Certain Measures Affecting Electronic Payment Services*, WT/DS413/R, adopted 31 August 2012.

Appellate Body Report, *Argentina - Measures Relating to Trade in Goods and Services*, WT/DS453/AB/R, adopted 9 May 2016.

Panel Report, *Russia-Measures Concerning Traffic in Transit*, WT/DS512/R, adopted 26 April 2019.