CHAPTER III

FINDING AND DISCUSSION

A. Finding

1. Data localization

a. Objectives of data localization

In the age where valuable information is kept on a series of codes which translates to a digital form of data, it is of great interests for States to secure its protection. States have differing objectives in applying data localization laws. However, there has been a common notion in describing data localization, which is as a protection of its "national resource." It is put in place as a means for States to protect its sovereignty and enforcement of laws over data that belongs to them. The forms in which it takes vary, data localization measures are not always seen within a clear legislation, in fact it may take the form of licencing provisions, contract requirements broadly created by public entities, and any requirements on data being transferred across border.

It must be distinguished that data localization is limited to the act of storing, processing, and collecting data within a State. It is the act of maintaining data within the residency of the data. The residency of data can be seen through the origin of the production of data. Such as data belonging the a certain national, or where the geographical location

in which the data was formed.[40] This stems off the desire of States to keep sensitive and important data, generally personal data, within the borders of their jurisdiction. In avoiding cross-border data flow, States are able to ensure that the laws and regulation will consistently apply at all times.

The few reasoning States apply data localization may include for purposes of data security and data privacy as a means to avoid cyber breaches of data. With no specific borders within the digital world, the only way to ensure the safety of data and the laws that applies is by keeping the data within physical servers in the State. In doing so, States are aware and has control over the physical location of the servers which holds the data, further having the ability to maintain and oversee the security level of such data. As mentioned above, data sovereignty may encompass the data to whom it belongs to,[41] the location of the sever which holds the data,[42] and the accessibility of the data.[43] In ensuring all points are covered, Stated resort to data localization laws.

Furthermore, economic consideration may be a reasoning States apply data localization laws as digital trade has grown exponentially over the years, holding an important role in the global trade. With the rise of digital trade, companies and States has great interest over digital

[40] Patrik Hummel, Matthias Braun, Max Tretter and Peter Dabrock, 'Data sovereignty: A review', Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. Big Data & Society, Vol. 8, Issue 1, doi:10.1177/2053951720982012, 6.
[41] Koops, *op. cit.,* 33.
[42] Koops, *op. cit.,* 27.
[43] Koops, *op. cit.,* 21.

data and how it is processed. Further increasing the concerns of States in ensuring the safety of such data.

Therefore, the differing reasoning States apply data localization laws, it can be concluded that they are all centred in the control and application of regulations over the data as well as the specific outcome targeted by the State.

b. Types of data localization

The right of States to regulate how data of belonging to its citizens and State must be processed – this is included with the concept of data sovereignty. These regulations encompass how data is processed within a State. Approaching the increase of digital data movement also

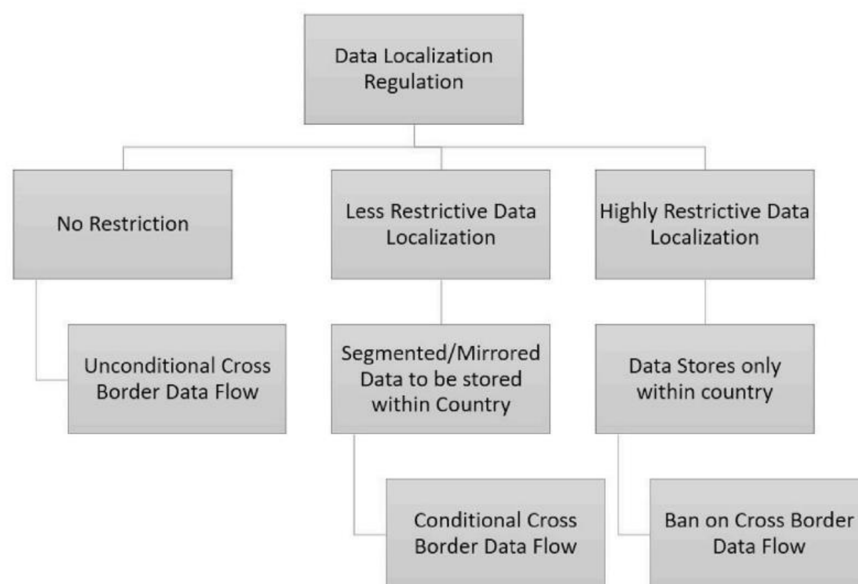

Figure 3. 1 Types of Data Localization Regulations

known as cross border data flow, States has taken different approaches in regulating such data. Hence, data localization arises through different forms and its manifestation has different effects. There are a variety of

data localization regulation, the most common types of data localization are divided into: (1) no restriction, (2) less strictive data localization, and (3) highly restrictive data localization.

(Source: Potluri, S. R., Sridhar, V., & Rao, S. (2020). Effects of data localization on digital trade: An agent-based modelling approach. Telecommunications Policy, 44)

1. No Restriction of data localization is where there are no data localization mandates by the States. This is seen in states such as Ireland and Iceland, these States allows a complete free flow of data between different jurisdictions. Creating a free and unconditional cross-border data flow.[44] Hence, all data can be easily transferred overseas.
2. Less restrictive data localization or relative data localization is when data may leave its jurisdiction in which the data resides in, however it may only be conducted under a predetermined set of circumstances. States with these types of data localization regulation allows cross-border transfer of data which helps entities to transfer data for specific purposes. As seen in States such as Australia and Thailand, cross-border data flow may only be conducted under strict requirements and for specific sectors. The general practice in less restrictive data localization laws is

[44] Martina Francesca Ferracane, et. al. *Digital trade restrictiveness* (2018) https://ecipe.org/wp-content/uploads/2018/05/DTRI_ FINAL.pdf., accessed on 26 February 2024.

for sensitive data to be stored within the home State, which include: health information, banking records, and other sensitive data.[45] As a result, this leads to a conditional cross border flow of data, in which cross border flow of data is allowed unless certain requirements has been fulfilled.

3. Highly restrictive data localization or referred to as absolute data localization is when data may not leave the jurisdiction in which it resides in, even if it's only temporarily. The State hold absolute and complete control over the data through data localization regulations. The stricter domestic laws regulate its data localization laws, the more security the data has within the State. These regulations are practiced by China, Russia, and Turkey. These States requires all data to be stored within the borders of their States. As a result, cross-border data flow is prohibited unless allowed for by the State.[46]

Therefore, in the different types of data localization, it can be further analysed the degree of strictness a State has towards the movement of data or cross border data flow within a State and its effects. The type of data localization State's implement may have differing effects.

c. Effects of data localization

[45] *Loc. cit.*
[46] *Loc. cit.*

Every action has consequences. In the implementation of data localization, consequences may vary depending on the degree and type of data localization is being implemented within the State. As explained above on the types of data localization, effects may occur in different aspects of digital trade.

Data localization creates barriers for service providers, and reducing investments. The most effected are local start-ups looking to attain the global market, restricting both the countries and start-ups.[47] However, simultaneously help local start up with local consumers. In the event that a State does not have any data localization restriction, the creation of a free-market flow opens up doors beyond borders and jurisdiction. A market can easily expand to a global level without any hindrance. There exists a producer at any moment which gives a competitive pricing and quality.[48]

However, when States implement data localization laws at different degrees of strictness, effects may be seen in a variety of ways. Such as: (1) competition between global and local producers, (2) effects on local economies, and (3) effects on competition and innovation.

Firstly, the effects on competition between global and locals can be seen drastically. A global firm targets a larger audience base

[47] S. R. Potluri, V. Sridhar & S. Rao, "Effects of data localization on digital trade: An agent-based modelling approach," *Telecommunications Policy* 44, no. 9, (2020) doi: 10.1016/j.telpol.2020.102022, accessed on 18 January 2024.
[48] *Loc. cit.*

globally, whereas a local firm targets consumer only within their home locations or the only within a specific geographic location. In research conducted by the International Institute of Information Technology Bangalore, the data localization restrictions were observed based on the average global market shares of local and global firms following 2 scenarios. First, a scenario where all countries does not have any data localization requirement, and second, a scenario where all countries have strict data localization laws. The result shows that in a scenario where all countries have highly restrictive data localization laws, local firms are able to obtain a much higher level of average global market share than it would in a scenario of no restriction on data localization laws. This is due to the fact that global firm would have a rigid restriction that it must follow increasing compliance cost. Therefore, despite limiting customers choices, customers prefer the local firms over the global firms. However, in the event that there exists no data localization restriction, markets became more competitive both for prices and quality as the local and global firms can compete equally with each other with the same level of restrictions.[49]

Second, the effects on local economies. It must be noted that in implementing a data localization restriction will simultaneously increase the compliance costs and inherently increase the price and quality of services towards producers from outside of the customer's

[49] *Ibid*, 9.

location. However, an opposite effect would occur towards local firms. As local producers are not subject to data localization restriction hence not effected by the compliance cost, the prices and quality are able to be maximized. Benefiting local firms, and allow them to thrive.[50]

Third, the effects on competition and innovation. A common practice conducted by digital firms is to collect data from users, which include purchased history, browsing patters, web sites visited, and even the extent of the cursor on the screen. In implementing data localization restriction, firms may be hindered to use such data from users, hence resulting in a decrease in quality and increase of price.[51]

The effects can play a big role in effecting the trade market of the international community. As understood, the sector that is mostly affected by data localization is e-commerce. E-commerce is a growth engine that is built on the basis of the free-flow of data. The continues increase of e-commerce is in line with the increase of the free flow of data. The dramatic increase of e-commerce has evolved to become an essential sector within trade. In 2016, the global retail market reached 1,548 trillion US dollars and in a span of 3 years, the number has doubled to become 3,53 trillion US dollars, leading to an increase in the overall portion within international retail. However, with the

[50] *Ibid*, 13.
[51] *Loc. cit.*

implementation of data localization, it would raise the barriers in the participation of the growing global market.

Hence, the effects of data localization can be seen a variety of ways both positively and negatively. It all comes down to the degree of and extend data localization laws is implemented by a State.

2. Trade barrier restrictions under the GATS

a. The objectives and purpose of trade barrier restrictions

Trade barriers are enacted for the purpose of protecting industries and workers within a State. This is seen through state practices where States implement restrictions for foreign products and services to show preference in domestic products and services. However, it does not hinder the fact that in some circumstances trade barrier is implemented as a political response or a retaliation towards another State's action.[52]

There are a variety of permissible trade barriers that is recognized in the international community. All trade barriers and its limitations are regulated in WTO's agreements, which include: (1) Tariffs which are tax on imports. Tax is the imposing of extra costs on a specific good that was brought into a country from another country, (2) quotas which are limits put on the amount of a certain good that can be imported from a certain country to another country, (3) embargoes

[52] Carr, Indira, *International Trade Law 4th Edition*, (New York: Routledge-Cavendish, 2010), 103.

which are a country's ban on trade with another country. This can be in the form of banning a specific good to be exported or include bans of all goods from a specific country, (4) standards which is the implementation of a specific criteria towards exported goods. The criteria may vary from health and safety criteria such as not allowing a specific type of pesticides use for crops, or even a certain criterion on labour conditions, and (5) subsidies which are direct payments given from the government towards producers of a certain good to be able to compete competitively with exported products.[53]

These types of trade barriers are permissible within the international community as long as it is implemented consistent with the limitations enshrined within international agreements. International agreements regulate on permissible trade barrier to create a fair trade in the international community for all participants of trade. It is further regulated to avoid State's from abusing its powers in its right to implement trade barriers within its jurisdiction.

Here in this paper, as the agreement that is used is the GATS, the GATS regulates on the limitations of trade to create a credible and reliable system of international trade rules, to ensure a fair and equitable treatment of all participants of international trade. In line with the objective of the GATS, its purpose is to stimulate economic activity

[53] Susan Ariel Aaronson and Patrick Leblond "Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO", *Journal of International Economic Law*, Oxford University Press, Vol. 21, 2018, 245.

through guaranteed polity bindings and promoting trade and development through progressive liberalization.

b. Trade barrier restrictions under the GATS

As an agreement under the WTO, the GATS regulates matters which concerns international trade on services. The GATS regulates on trade barrier limitation, and certain grounds that may not be violated in implementing trade barriers.

The GATS regulates on its limitations thoroughly and strictly. Here, are the major limitations in implementing trade barriers that must not be violated. The following rules include:

1. *National treatment*: Article XVII of GATS provides that Members have to accord to services and service suppliers of any other Member, "treatment no less favourable than it accords to its own like services and service suppliers."
2. *Market access*: Article XVI:2 of GATS provides a list of market access commitments to be complied by Members in sectors where market access commitments are undertaken. As per Article XVI:2 (a) Members will not adopt measures which impose 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.
3. *General exception*: Article XIV of GATS regulates on an exception that a State may implement trade barriers if it is for the purpose of

"necessary to protect public morals or to maintain public order or to protect human, animal, or plant life and health, or for the compliance of a law or regulation that is not inconsistent with the GATS." This article is implemented under serious conditions that it is necessary to protect matters as mentioned within the article.

4. *Security exception*: Article XIV bis of GATS regulates on the exceptions that a State may implement if it is "necessary for the protection of its essential security interest, which includes: the supply of services for the purpose of provisioning its military establishment, or relating to fissionable materials from which they are derived, and or in times of war or other emergency in international relations." To obtain the rights to establish such measures under this article, State party must inform the council of trade under the WTO to the fullest extent possible of the measures taken.

The aforementioned articles regulate on the main regulations that must be adhered to strictly in the event a State wishes to implement data localization law. As explained before, though not explicitly specified, the GATS does encompass its regulation to include digital trade. The WTO has defined electronic commerce as the production, distribution, marketing, sale or delivery of goods and services by

electronic means.[54] Hence, these limitations do extent towards international digital trade.

c. Practices of data localization in the international community

States apply data localization in a variety of ways and with different degrees. Different States apply different forms of data localization and for different reasonings. Below are the different ways States implement data localization law. Below are the different States who has applied data localization laws within their State in a variety of degrees.

1. Turkey – Amendments to the regulation of Internet Broadcasts and Prevention of Crimes Committed through such Broadcasts, also known as the social media Law in Turkey. This Turkish law defined the term social network provider to a legal person that provide opportunities for users to create, view, or share data for social interaction online, a broad definition which encompasses a variety of companies. The law requires domestic and foreign social network provider to store user data within Turkey's territory following a report every 6 months. This includes all citizen within its country.
2. Russia –Federal Law No. 242-FZ is a law that aims to protect Russian citizen's data by keeping it inside of Russia. Furthermore, the law further regulates that personal information

[54] WTO, *Op. cit.,* 35.

can only be collected for specific purposes and must have been stated in advance. The collection of personal data must be stored in databases inside of Russia. Requiring all companies to have servers within Russia.

3. India – The (Indian) Companies Act 2013 and the Companies (Accounts) Rules 2014 Section 94 with in conjunction with sections 88 and 92, require covered organizations to store financial information at the registered office of the company. Furthermore, The Reserve Bank of India's Directive 2017-18/153 issued under the Payment and Settlement Systems Act 2007 paragraph 2 (i) of the Directive requires covered organizations to store payment data within India. Lastly, The IRDAI or Maintenance of Insurance Records Regulation 2015 paragraph 3(9) requires covered organizations to store insurance data within India.

4. China – China data protection laws have set specific requirements for cross-border data transfer by companies that collect Chinese citizens' personal information. The China Personal Information Protection Law (PIPL) compliance, to which companies are expected to keep data collected and processed in China within Chinese borders. Furthermore, specific provisions of China's data residency laws do allow for cross-border data transfer, under strict requirements that must be

met. One of which specifies that businesses use cloud services in China to store the personal information of Chinese citizens.

5. Indonesia –Government Regulation No. 71 of 2019 on Electronic Systems and Transactions requires private operators to choose whether to process or store their electronic systems and data within or outside of Indonesia's jurisdiction. Regardless of the location, the Indonesian government obliges companies to ensure that their electronic systems and data are accessible to Indonesian authority at all times or upon a request. Hence any Foreign companies who wish to provide services in Indonesia are allowed to keep data within its territory as long as it is consistent with data protection requirements within Indonesia. However, this flexibility does not apply to private operators in the banking and financial services sectors, as they are subject to sector-specific laws and regulations, depending on the type of financial institution.

These are the few States that implement data localization regulations. These states apply data localization laws at a different degree and in different sector of the digital field. Despite the differences all states have one thing in common which is which is the fact that it regulates on how data should be processed within their state prior to cross border transfers.

B. Discussion

1. The extent States implement data localization and its impacts trade barrier

As digital trade continues to expands, States are facing dilemmas between expanding opportunities originating from digital trade by allowing free flow of data, which is essential for innovation and economic growth in the digital world, and, on the other, to managing the impact of cross-border data flows for other interests, which include privacy and cybersecurity. Due to conflicting interest, it has resulted in a complex domestic legal landscape for digital trade.[55]

In practice within the international community, States have different ways in applying data localization laws. As discussed above, there are different types of data localization laws, which include: (1) no restriction, (2) less strictive data localization, and (3) highly restrictive data localization. The differences in strictness of data localization requirement, would result to different effects.

It must further be understood on the events to which a data localization requirement would amount to a trade barrier inconsistent with GATS restrictions, and how data localization has been practiced within the international community.

a. Inconsistencies of Data Localization with GATS restrictions

[55] Meltzer, *loc.cit.*

The excessive implementation of domestic regulation in protecting cross-border data flow may lead to disadvantages towards services that is unnecessary and disproportionate to fulfil its domestic interest and objectives. Extreme standards and overreaching data protection requirement could seriously impact trade negatively the digital market, similar to the effects of tariffs, quotas, and other protective measures that can be seen within traditional forms of trade.[56]

As understood above, the GATS regulates on limitations towards trade barriers which regulates strict rules. The limitations are set with a certain threshold, which are:

1. *National treatment*: Article XVII of GATS provides that Members have to accord to services and service suppliers of any other Member, "treatment no less favourable than it accords to its own like services and service suppliers." The requirement that is put forth within this article is for States to not discriminatorily apply barriers for the purpose of benefiting domestic services and suppliers.

In *China - Certain Measures Affecting Electronic Payment Services*, the panel used a three-part test assessment in determining a violation of article XVII.[57] The assessment include, 1) the state has

[56] C.L. Lim, Deborah Elms, and Patrick Low, "The Trans-Pacific Partnership: A Quest for a 21st Century Trade Agreement," *Cambridge University Press* (November, 2012): 171.
[57] *China - Certain Measures Affecting Electronic Payment Services*, https://www.wto.org/english/tratop_e/dispu_e/413r_a_e.doc, accessed on 17 February 2024.

made a commitment on national treatment in the relevant sector and mode of supply, 2) the measures are affecting the supply of services in the relevant sector and mode of supply, and 3) the measures that are put in place to services or service suppliers of any other member State treatment less favourable than it accords its own like services and service suppliers.

With all things considered, data localization measures affect the supply of services within a particular sector, it would most definitely violate a member's national treatment obligation. This is due to the fact that the effects of data localization would require foreign services or suppliers to follow such localization requirements by having an expensive local infrastructure, increasing their costs, and resulting in a less favourable treatment than domestic suppliers.

2. *Market access*: Article XVI:2 of GATS provides a list of market access commitments that must be complied with by the Members in a specific sector where market access commitments are undertaken. As regulated under Article XVI:2 (a) Members will not adopt measures which impose 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. This rule requires State to maintain its commitments for market access that has been established. Within *US-Gambling*, the

WTO appellate body found US' laws in prohibiting cross-border supply of gambling and betting services as inconsistent with Article XVI:2 (a) on the basis that a prohibition towards one, several, or all means of cross-border delivery is a direct limitation on the number of services suppliers in the form of numerical quotas within the definition national treatment under GATS as it completely prevents the use of service suppliers of one, several or all means of delivery that are included. In terms of data localization, it may be argued that data localization measures are a direct limitation on the number of services suppliers as it completely prevents the use by service suppliers of one, several or all means of delivery of cross-border digital service.[58]

3. *General exception*: Article XIV of GATS regulates on an exception that a State may implement trade barriers if it is consistent with the general exceptions. There exist two requirements: article XIV (a) and XIV (c).

   First, article XIV (a) regulates on measures that is necessary to protect public morals or to maintain public order. Within this article, States are under the obligation to prove the necessity of adopting such a measure to achieve its objectives. Under WTO's jurisprudence, this encompasses weighing and balancing test. This

[58] *United States — Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm, accessed on 17 February 2024.

is proven with three tests: first, the contribution of the measure to achieve a legitimate objective either for public moral or public order; Second, it must be put into consideration the restrictive impact of the measure towards international commerce; and lastly, the if there are other less restrictive measures that may achieve the legitimate purpose. Furthermore, the scope of Article XIV(a) further includes "public order exception may be invoked only where a genuine and sufficiently serious threat is posed to one of the fundamental interests of society." As a result, any State seeking to justify measures of data localization under this exception will have to fulfil the high threshold of the 'weighing and balancing' test and 'public order'.

Second, a State may justify implementing measures inconsistent with the GATS for the purpose of circumstances which include: (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. Under this requirement, it is much more suitable to be used as a justification in the application of data localization for States. However, the 'weighing and balancing' test will have to be fulfilled even under this exception as mentioned under article XIV (a).

4. *Security exception*: Article XIV bis of GATS regulates on the exceptions that a State may implement if it is "necessary for the protection of its essential security interest, which includes: the supply of services for the purpose of provisioning its military establishment, or relating to fissionable materials from which they are derived, and or in times of war or other emergency in international relations." To obtain the rights to establish such measures under this article, State party must inform the council of trade under the WTO to the fullest extent possible of the measures taken.

After understanding how the limitations on trade barriers stated within the GATS applies within data localization regulation. This paper will further dive deeper on how such data localization regulation is applied within by international community.

b. Practices of data localization amounting to a trade barrier

There are a variety of ways State implement data localization. Here within this discussion, the writer will look further into the application within 5 different States. Below is the explanation:

Table 3. 1 Legality of Data Localization with GATS

No.	State	Data localization Requirement	GATS violation
1.	Turkey	The law requires domestic and	Article XVII National Treatment

		foreign social network provider to store user data within Turkey's territory following a report every 6 months. This includes all citizen within its country.	The WTO panel has analysed the application article XVII in *China - Certain Measures Affecting Electronic Payment Services* by using a three-part test assessment.[59] Here, the three-part test has been fulfilled as Turkey has made no limitations on the national treatment rule in its schedule regarding this sector, the application of its data localization effects the supply of services in the sector, and given the burden it puts against foreign service providers, it amounts to a less favourable treatment. Given the nature of the requirement of obliging companies to store data within the territory of Turkey creates a disproportionate burden towards foreign companies. As it would greatly increase the cost for foreign companies to create servers within Turkey. This directly creates an advantage towards local companies.
			Article XVI:2 Market Access The complete obligation to store data within Turkey directly hinders the ability of foreign companies to enter without owning a server within Turkey.

[59] *Loc. cit.*

			As seen in *US- Gambling*, a complete ban of cross-border supply of gambling and betting services is inconsistent with market access under the GATS. Similarly here, a complete obligation towards all data to be stored within Turkey, hinders the access of market towards foreign companies.
			Article XIV General Exception In order to fulfil the necessity test, it must be the only way to achieve the legitimate aim. In *US – Gambling*, this requires that the challenged measure address the particular interest specified in that paragraph and that there be a sufficient relation between the measure and the interest protected, or in other words there must be a degree of connection between the aim and the action pursued. Here, requiring companies to store data within the territory of Turkey and further requesting a report on their citizens data is extensive, if the aim is for the purpose of protecting their citizen's data, as merely requesting for a report is sufficient to achieve the aims. There exists no reasoning why a complete request of storing the data

			within Turkey is the only way it would guarantee the protection.
			Article XIV Security Exception If a State would to rely on security exception as a precluding of wrongfulness under the GATS, the State must submit to the WTO panel a request for such article to apply. However, in the event the State has submitted a letter towards the WTO panel it must be done only if it is necessary for the protection of its essential security interest, which includes: the supply of services for the purpose of provisioning its military establishment, or relating to fissionable materials from which they are derived, and or in times of war or other emergency in international relations. Here, such circumstances have not been fulfilled. Therefore, Turkey may not rely on the article on security exception.
2.	Russia	The collection of personal data must be stored in databases inside of Russia.	Article XVII National Treatment Given the nature of the requirement store data within the territory of Russia creates a disproportionate burden

		Requiring all companies to have servers within Russia.	towards foreign companies. As it would greatly increase the cost for foreign companies to create servers within Russia. This directly creates an advantage towards local companies.
			Article XVI:2 Market Access In a claim brought by the United States against Japan titled *Japan – Measures Affecting Distribution Services*, the United States had claimed that Japan's measures on the regulating retail stores floor space, business hours and holidays of supermarkets and department stores were a violation of the market access clause under the GATS.[60] Similarly here, it may be argued that a complete obligation to store data within Russia directly burdens and hinders the ability of foreign companies to enter without owning a server within Russia. Limiting the market access towards local companies. This can directly be seen as Linked in could not operate within Russia given the extent of its data localization requirement.
			Article XIV General Exception

[60] *Japan — Measures Affecting Distribution Services*, https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds45_e.htm, accessed on 18 February 2024.

			Forcing companies to store data within the territory of Russia and further requesting a report on their citizens data is extensive to merely "protect the citizen's data" as other measures such as making sure that the pre-existing servers of digital companies have met the minimum requirement for of safety would have been sufficient.
			Article XIV Security Exception Does not apply as this article is only applicable for an essential security interest, which includes: the supply of services for the purpose of provisioning its military establishment, or relating to fissionable materials from which they are derived, and or in times of war or other emergency in international relations.
3.	India	Data in relation to financial information must be stored within India. Furthermore, it requires organizations to store payment data within India.	Article XVII National Treatment The obligation to store data within the territory of India within a specific sector would still amount to the violation of the national treatment clause as it creates a disproportionate burden towards foreign companies. In the case of *Belgium — Measures Affecting Commercial Telephone Directory*

			Services' the regulations applied by Belgium on obtaining a license to public directories, and other regulations in relation to telephone directories was inconsistent with article XVII of the GATS.[61] Here, it may be argued that having to store data within India and further work with an Indian institution is inconsistent with article XVII of the GATS. This has been seen towards certain banks that is struggling to maintain itself within India as a result of its data localization requirement.
			Article XVI:2 Market Access A hindrance towards market access is a violation of this clause. As has been emphasised in *US – Gambling* case, a complete ban on specific services is a violation of the market access clause. Here, the fact that all digital payments must be processed in India equates to a complete ban of a specific services as seen in the *US – Gambling case*. In India, this can be seen as certain banks that is struggling to maintain itself is an

[61] *Belgium — Measures Affecting Commercial Telephone Directory Services*, https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds80_e.htm, accessed on 20 February 2024.

<table>
<tr><td rowspan="3"></td><td rowspan="3"></td><td rowspan="3"></td><td>inconsistency towards the market access clause within the GATS.</td></tr>
<tr><td>Article XIV
General Exception
The necessity test may be argued to have been fulfilled as the localization requirement is created towards specific sectors instead of applying data localization towards all sectors.</td></tr>
<tr><td>Article XIV
Security Exception
Does not apply as this article is only applicable for an essential security interest, which includes: the supply of services for the purpose of provisioning its military establishment, or relating to fissionable materials from which they are derived, and or in times of war or other emergency in international relations</td></tr>
<tr><td rowspan="2">4.</td><td rowspan="2">China</td><td rowspan="2">Companies are expected to keep data collected and processed in China within Chinese borders. Furthermore, specific provisions of China’s data</td><td>Article XVII
National Treatment
An obligation to store data within the territory of China and further using the cloud within China would directly impact foreign companies.</td></tr>
<tr><td>Article XVI:2
Market Access
The nature of China’s data localization laws has led to the point where only</td></tr>
</table>

		residency laws do allow for cross-border data transfer, under strict requirements that must be met. One of which specifies that businesses use cloud services in China to store the personal information of Chinese citizens.	Chinese companies is dominant within China. As it is almost impossible to penetrate the market within China. This is a direct violation of the market access clause within the GATS.
			Article XIV General Exception There exists no necessity is implementing a regulation this strict towards data. It is not the least intrusive means to achieve the legitimate purpose.
			Article XIV Security Exception Does not apply as this article is only applicable for an essential security interest, which includes: the supply of services for the purpose of provisioning its military establishment, or relating to fissionable materials from which they are derived, and or in times of war or other emergency in international relations
5.	Indonesia	The requirement for private operators to choose whether to process or store their electronic systems and data within or outside	Article XVII National Treatment Indonesia no longer obliges private companies to have a server located within the territory of Indonesia, however, Indonesia require that all foreign companies meet the minimum standard of data protection as regulated

		of Indonesia's jurisdiction as long as it meets the data protection requirement.	in Indonesia. This violates the national treatment clause as only foreign companies are subject to this rule, whereas local companies are more lenient to this rule.
			Article XVI:2 Market Access Given the ability of foreign companies to be able to store its data abroad, and is no longer required to have a data server within Indonesia, it creates an open market that is not heavily burdensome towards foreign companies.
			Article XIV General Exception The necessity test may be argued to have been fulfilled as the localization requirement is created towards private sectors instead of applying data localization towards all sectors.
			Article XIV Security Exception Does not apply as this article is only applicable for an essential security interest, which includes: the supply of services for the purpose of provisioning its military establishment, or relating to fissionable materials from which they are derived, and or in times of war or

			other emergency in international relations

Table 1: The comparison of how States Apply Data Localization Laws and Its Compatibility with the GATS

As understood above, the different ways States implement data localization laws, effects the international communities and violated the regulation under the WTO differently. However, a pattern that can be seen is a general violation occurs in the national treatment and market access clause. In situation where States are obligated to have a server within the State, it creates a violation for national treatment and market access as it over burdens foreign companies. However, in situations where states are more specific, such as a requirement for sector specific services are obligated to follow data localization requirement tend to now violate the market access clause. It can be inferred that the strictness of a data localization can affects its consistencies with the GATS.

As a result, this paper will further discuss on ways to overcome such violations under the GATS.

2. Overcome data localization as an impermissible trade

a. Applying the restrictions under the GATS towards digital trade

The importance of applying the GATS towards digital trade would help in maintaining the consistency within digital trade. As has been explained above, though not explicitly specified, the GATS does encompass its regulation to include digital trade.

As WTO has defined electronic commerce as the production, distribution, marketing, sale or delivery of goods and services by electronic means.[62] It has established that any forms of distribution, marketing, sale or delivers of goods and services whether through traditional or electronical does incurs the application of the GATS. Given the rise of digital trade and the continuously growing market on the internet, the acknowledgement of such forms of trade by the WTO requires digital trade to be consistent with WTO agreements.

Thus, as trade barriers regulation within the GATS does extend towards digital trade barriers. In practice, he application of trade barriers in digital trade may differ in its form, however, the rules and principle still apply. With States acknowledging that the GATS applies towards digital, would maintain the consistency in digital trade.

In terms of national treatment, States may avoid violations by providing an equal treatment for both domestic and foreign services. This may be conducted by enforcing all service providers to provide a report of data collected towards the government and allowing them to use their pre-existing servers. Furthermore, in regards to market access, States must allow the existing foreign service providers to enter its domestic market without and hindrance. Lastly, any request for exceptions must be applied carefully, and fulfil all existing threshold.

b. Creating a Digital Trade Agreements

[62] WTO, *op. cit.*, 35.

Just as States creates agreements between each other for cooperation in trade, States must now further create digital trade agreement. Digital trade agreement has been rising in the past few years. As seen between the European Union and South Korea as well as Singapore to further expand opportunities within digital trade.[63]

Digital trade agreements cover trade in goods and services that are enabled by the internet or through digital platforms, and other information and communication technologies. Digital trade regulates a variety of goods or services ordered digitally and physically delivered, for example, ordering clothes online that that will be delivered to your house, or goods or services ordered digitally and delivered digitally, for example buying an app that you install on your smartphone. It further encompasses any goods and services that uses of technologies in production or distribution processes, for example tracking road cargo in real time to develop more efficient supply chains or the transfer of data across borders for example data stored in the cloud when working online.[64]

With the existence of digital trade agreements, it further helps to unlock new markets that offer a wide choice of high qualities of goods and services that can easily be found and procured online. States

[63] Kim, Minjung, *Unlocking the Potential of Digital Services Trade in Asia and the Pacific*, (Asian Development Bank, 2022), 156.
[64] European Commision, "Digital Tade Agreements", https://policy.trade.ec.europa.eu/help-exporters-and-importers/accessing-markets/goods-and-services/digital-trade/digital-trade-agreements_en, accessed on 29 March 2023.

that enter into an agreement in regards to digital trade opens up barriers to further enhance digital trade. These agreements makes electronic transactions easier, promotes a safe online environment for consumers, ensures consumer protection, and protecting consumers' data, creating legal certainty for businesses and boosting trust, for example, no data localisation requirements, protection of computer source code, avoiding forced technology transfer, improving access to electronic commerce, and lastly provide digital trade facilities, such as less administrative burden for electronic commerce, for example paperless trading, e-invoicing.

With the existence of trade agreements, it creates a reference for States to conduct trade with each other. Creating a trading environment that is beneficial for the signing States. Furthermore, an agreement between States would further minimize any data localization that would affect the trading parties.

c. Creating a Free Trade Agreements

As States enter into agreements to further enhance digital trade, a free trade agreement is another way to combat digital trade barriers. A free trade agreement is an agreement between two or more States who agree on certain obligations that affect trade in goods and services,

and protections for investors and intellectual property rights, among other topics.[65]

Free trade agreements for digital trade have begun to be implemented by States. For example, the United States and Australia has entered into a free trade agreement specifically between within digital trade. The agreement between the United States and Australia has stated that it recognises the economic growth and opportunity that electronic commerce provides, the importance of avoiding barriers to its use and development, and the applicability of the WTO Agreement to measures affecting electronic commerce.

As practiced by United States and Australia, and among other countries. It shows that free trade agreements between States can be conducted within digital trade to create a better and free environment even within the digital world.

d. Creating a balance between government interest and the international community

As has been understood, the concept of international trade refers to all economic activities for international cross-border exchange of goods and services. These activities expand to a variety of sectors, from raw materials or finished goods, to further include various types of services, from financial services to tourism and lastly and most recently

[65] Mira Burri, "Towards a New Treaty on Digital Trade". *Journal of World Trade* 55, no. 1 (2021), 78.

being developed, is the digital services. Digital services come in a variety of forms. Today, the digital trade has evolved to having an important role within international trade. Given the interconnectedness of the digital world, digital trade now holds a key role in driving the global economic growth.

With digital economy continuously developing, problems and concerns from States has simultaneously arise. The intangible nature of data that is able to be accessed cross-borders making territory irrelevant, raises the concerns of States to conduct measures that protects the cross-border transfer of data and the data of its citizens.

Which leads to the dilemma that States has towards the internet and digital trade. The main concern at risk in regards to digital data are data breaches and cybersecurity issues. With the nature of digital economy, the need for the transfer of data cross-border has become an integral part in today’s digital trade. It is shown through how the internet works today, a person can send an email from their State to another person located in a different State, to which the email can be opened from anywhere in the world as long as there is internet access. Across the board, cross-border of data is needed for the fast pace world we live in today.

As a result, States are constantly in conflict in protecting the citizen's data from any cyber-attacks and being misused by third party entities whilst also having the interest of increasing and continuously

developing international digital trade. It is of great importance to find a balance between protecting data and also protecting the digital trade.

In finding a balance, States must put into consideration the extent that they want to protect their citizens data and finding the necessary and proportional measure to be able to fulfil that goal. The emphasis is put in adopting the least intrusive means without compromising of jeopardizing any interest at state. In implementing this measure, states can both protect their citizen's data whilst simultaneously still encourage digital trade. Underlining the most important aspects that must be protected and of greatest interest, and further finding the middle ground.

These acts can be seen through State practice in implementing limited data localization. For example, in terms of national treatment. Given the obligation not to put forth a treatment less favourable to its own like services, in substitution with data localization requirements, States may conduct the measure of submitting a report after a certain period of time. This way, the national treatment clause under the GATS is not violated.

Furthermore, negotiations can be conducted between States to find a middle ground in regards to the extent they would like to regulate their trade on services. As regulated under article XIX of the GATS, members in advised to enter into successive rounds of negotiations to improve their schedules of specific commitments. This is one of the best

ways to avoid any conflicts of interest, as a negotiation could lead to an agreement which acts as a reference for future conducts on trade.

Nonetheless, all things must be considered in finding a balance between national interest and the international community’s interest.