CHAPTER II

LITERATURE REVIEW

A. General Review on Digital Data

1. Review on Data

Data is defined and regulated different depending on the State. There are a variety of definition on data that is used today. It must be put into consideration, due to its vague definition, there exists no consistent practice on how States regulates data. The reasoning to the major importance of data is seen through the broad usage of data. Within data, there are information, and through information there is knowledge.[12] A common definition of data is established by Checkland and Holwell in 1998 which defined data as: "Data: A representation of facts, concepts or instructions in a formalised manner suitable for communication, interpretation, or processing by humans or by automatic means."[13]

As the aforementioned quote has mentioned that data is used in a communicative, interpretive and processing means reflects the variety of means that data may be utilized. Data can be a powerful tool depending on the hands that it lies on. As time progresses, data has now shifted to exist within the digital world. Hence both physical and digital data must be heavily regulated on its protection.

[12] Cambridge International AS & A Level Information Technology 9626, Topic 1.1 Data (Cambridge International Examinations, 2015), 5.
[13] Narendra Gupta et al., "Maintenance and analysis of agricultural data: a challenge", *International Journal of Bioassays* 5, no. 9 (2016): 4842-4848.

The nature of digital data holds a similar weight to a traditional physical form of data, however its nature in the physical world is different. Data takes a more intricate form, it is a combination of codes in a binary format using a series of numbers that is digitally processed, stored, and further transmitted by electronic devices.[14] As a result, digital data can translate to all sorts of valuable data. However, with its digital nature, and no physical form, digital data raises concerns on the sovereignty and jurisdictional aspect. Digital data may be accessed at anytime and anywhere. The transborder nature of data raises the concerns for States to pursue steps in order to avoid crimes within cyberspaces.

Hence due to data's intricate nature, it has resulted in continues debates on the legality of certain regulation. Here within this section, the writer will further discuss on the general view of data in the digital world, data sovereignty, the concerns on cybersecurity, along with its protection for individual and trade purposes.

2. Review on The Digital Economy

With the continues advance of digital data, the use of data varies and how now been a big part of the economy. The digital economy is the economic activity that is created through billions of people, businesses, devices, and data being connected online. The centre of digital economy is the internet that connects people in different ways. As digital economy is

[14] Edward Elgar, "Digital Data and Methods," *Research Handbook on Analytical Sociology*, (2021): 352-363, DOI:10.4337/9781789906851.00028, accessed on 19 January 2024.

taking shape and undermining convention forms of how traditional businesses are structured and its interaction with the customers.[15]

In a globalized world, digital economy has opened up borders for countries to penetrate in expanding its revenue. It has created a broad opportunity that encourages innovations in their product and services, access to market intelligence, talent, financing and increasing competitiveness in local and global market.

At the heart of digital economy, is the advancement of technology. The tech industry is constantly pushing boundaries to enhance its market further. A digital trade is not limited to buying and selling goods and services on the internet, it further includes the transmission of information and data across borders. It relies on the use of digital technologies to facilitate trade and improve productivity.

Digital economy comes in different forms, e-commerce, social commerce, and social network provider. E-commerce is the act of buying and selling goods and services, or the transmitting of funds or data through electronic means. Social commerce is the act of promoting goods and services that it provides through the internet. All these points, are created through a social network provider. In the midst of digital economy, social network creates a platform that people from all walks of life are able to access. It connects the world through its platform, both for commercial and

[15] Deloitte, "What is Digital Economy," 2023, https://www2.deloitte.com/mt/en/pages/technology/articles/mt-what-is-digital-economy.html, accessed on 30 January 2024.

social purposes. In order to connect and use these platforms, personal data of users are held by social media network providers, which contains sensitive personal information. Commonly required data are names, age, data of birth, country of origin, gender, bank accounts, and other sensitive information.

According to the General Data Protection Regulation (GDPR), personal data is defined as any information in relation to the identity or it is identifiable to a natural person. An identifiable natural person is one who can be identified either directly or indirectly such as through name, identification number, location data, an online identifier or to other factors that may be attributed to a certain natural person. With the powerful nature of data, great due care must be put in its protection. The manifestation of its protection may vary.

With digital economy continuously developing, problems and concerns from States has simultaneously arise. The intangible form of data that is able to be access cross-borders making territory irrelevant has raised the question in regards to sovereign and how states should protect its national's data.[16]

3. Review on Data Sovereignty and Data Protection

With the rise of digital economy, the nature of cross-border data flow where a data can be accessed anywhere at any time in the world raises

[16] Handbook on Measuring Digital Trade Second Edition, (Geneva: The International Monetary Fund, the Organisation for Economic Co-operation and Development, the United Nations and the World Trade Organization, 2023), 15.

State's interest in the protection and cybersecurity risks of its national's data. However, due to its intangible nature that involves more than one jurisdiction, States must establish its sovereign rights over the data in order to apply its laws to protect the data of its nationals from cybersecurity concerns.[17]

The principle of sovereignty has been recognized as a principle of international law, and plays a big part within the international community. [18] Sovereignty is recognized as the exclusive right to exercise complete authority over legislative, judicial, and executive matters within its jurisdiction. Jurisdiction refers to the right of States of applying its laws towards object, situations, and persons.[19] The concept of sovereignty and jurisdiction must be understood conjointly as sovereignty lies in the power to exercise its authority without limitation or intervention from other entities, whilst jurisdiction is specified to the ability of States to apply its laws. It must be further understood that the ability to make laws is essentially the idea behind sovereignty.[20]

In its application of jurisdiction, overlapping may occur which would result into international friction. Hence, within the context of globalization, the understanding of sovereignty and jurisdiction must be understood

[17] Wu, Emily, *Sovereignty and Data Localization* (Harvard Kennedy School, 2021), 9.
[18] *Island of Palmas* (*USA v. Netherlands*), https://legal.un.org/riaa/cases/vol_II/829-871.pdf, accessed on 11 Februrary 2024.
[19] C.M.J Ryngaert, "The Concept of Jurisdiction in International Law Cedric Ryngaert", *Research Handbooks in International Law series* (2015): 50-76.
[20] Bhala, Raj, International Trade Law: A Comprehensive Textbook, (The University of Kansas, 2019).

conjointly with the interest of the international community. In its application of achieving the common goal of international peace requires international cooperation.[21]

As it has been understood that the definition of sovereignty – the supreme authority of every State within its territory to the exclusion of other States – is undisputed, jurisdiction may vary in its application and types. There are 2 types of jurisdictions, prescriptive jurisdiction and enforcement jurisdiction. Prescriptive jurisdiction is the power to regulate a certain activity, and enforcement jurisdiction is the ability for a State to lawfully exercise its laws through law enforcements pursuant to the domestic law of the State.[22]

Furthermore, jurisdiction can be further categorized based on the nationality of either the perpetrator or the victim, the territory, and the ownership of a certain object. In the traditional sense, jurisdiction can be easily identified and tracked down on the State that has the jurisdiction over a certain matter. For example, in terms of embassies, though located in a foreign State, the building itself still falls within the jurisdiction of the State of the embassy in which it belongs to.[23] However, debates begin to arise within the digital world, where the location, accessibility, storage,

[21] Ramona Gabriela Tatar and Adela Moisi, "The Concept of Sovereignty," *Journal of Public Administration, Finance and Law*, Issue 24 (2022): 292, https://doi.org/10.47743/jopafl-2022-24-27.
[22] D. Rothwell, S. Kaye, A. Akhtarkhavari, & R. Davis "Jurisdiction, International Law," *Cambridge University Press* (2010): 294, doi:10.1017/cbo9780511997341.008.
[23] Areas of Jurisdiction of ITPC LA (Kementrian Luar Negeri Republik Indonesia) https://kemlu.go.id/losangeles/en/read/areas-of-jurisdiction-of-itpc-la/3304/etc-menu, accessed on 17 February 2024.

ownership may involve more than one State, hence more than a single jurisdiction.

In respect to digital data, the infrastructure that creates a digital data varies. The main concern that creates a contentious debate revolves around, the location of the server, the accessibility of the data, and owner of the data. The contention arises due to the overlapping jurisdiction that occurs. The borderless nature of data creates difficulties on the division of jurisdiction over a data.[24]

These continuous contention on jurisdiction follows the traditional concept of sovereignty and converts the concept that is recognized in international law to apply towards data in the digital realm. As the principle of sovereignty extends towards data within a State. A State has sovereignty over the data of their people and the data within their jurisdiction. Therefore, State sovereignty applies to computer related activities and over computer infrastructure within their territory.[25]

In regards to computer infrastructure internally and physically, there are aspects that must be differentiated. Especially in terms of people's personal data. In regulating personal data, we must take into account: (a) the data to

[24] Milton L. Mueller, "Against Sovereignty in Cyberspace," *International Studies Review* 22, Issue 4 (2020): 2.
[25] Report of the Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (United Nations General Assembly, A/70/174, July 2015).

whom it belongs to,[26] (b) the location of the sever which holds the data,[27] and (c) the accessibility of the data.[28]

a. The owner of the data

The data to whom it belongs to plays a major role in determining who has jurisdiction. Following the concept of nationality jurisdiction, a State has the ability to control their nationals. This includes data that belongs to their nationals. State has jurisdiction and the obligation to control as well as protecting their national's data.

b. The location of the server

The location of the server determines the precise location of data as it is the physical infrastructure of the data. The physical location further determines the State that has jurisdiction. As understood, territorial jurisdiction is the most common form in determining jurisdiction of a State. Once the location has been determined, territorial sovereignty determines which State has jurisdiction. Any attempt to collect data from a server located outside of its territory without any prior consent of the State's in which the data is located would amount to a breach of territorial integrity and international law.

c. The accessibility of data

[26] Bert-Jaap Koops and Morag Goodwin, "Cyberspace, the cloud, and cross-border, criminal investigation, The limits and possibilities of international law," *Tilburg Law Research Paper* (December, 2014): 33.
[27] *Ibid*, 27.
[28] *Ibid*, 21.

The accessibility of data can further be used as a consideration in determining a State's jurisdiction. The ability to access data is the most contentious aspect for data. Today's interconnected world has opened doors and barriers in accessing data. The borderless nature of the accessibility of data is highly connected to the location of server, as the server is what holds these data. Therefore, State pays great attention in who can access these data and must involve high due care. It is still under continues debate if the State that has the ability to access data from its territory has jurisdiction over the data. However, the accessibility is still used as consideration of who has jurisdiction.

The aforementioned aspects of data are what States continuously dispute on. Given the interest that States has to protect its national's data, one way to protect such data is through the establishment of sovereignty and jurisdiction over these data. However, the overlapping jurisdiction is what further creates overlapping in laws and regulations. As a result, the most impacted sector is the trade sector. Further within this paper, the writer will discuss the corelation between sovereignty and how it acts as a dispute towards data localization as States still has an interest in the protection of data of its nationals.

4. Review on Cybersecurity and Data Protection

The Rapid growth in technology and the continuous advancements of digital data has enhanced the scope of data crimes around the world. The improvement of the internet has connected the world and penetrating

through all geographical boundaries.[29] Which further increases the risks of cybersecurity. With social network providers holding sensitive data of people. States now has the interest to protect these data.

As fast as the digital world grew, the hacking world grew faster. There are two ways of looking at the issue of cybersecurity specifically in relation to personal data. One is through the law and second is viewed through the physical data security that the entities holding the data – generally companies or the State – to protect the data.

First, the law has the ability to regulate crimes within the cyber world. The more intricate the law provides on cyber spaces, the better cyberspaces become. The law is the first step in protecting cyberspaces. The use of cyber security through laws can help minimize cyber-attacks, data breaches and identity theft and can aid in risk management. It has the ability to provide consequences and a specific due process in avoiding crimes within cyberspaces. With strict regulations on how digital data should be kept, it will result in a legally binding obligation both for the State and for companies to take the extra step in making sure that its data is well protected.

Second, in a computing context, security comprises cyber security and physical security which are both used by enterprises as a safeguard against unauthorized access to data centres and other computerized systems.

[29] Koento Pinandito N Irianto, "Digital Asset And Personal Data Protection In The Metaverse: Analyzing The Implementation Of Indonesian Laws In Addressing Challenges In The Virtual Era", *Indonesian Law Journal* 16, no 2, (December, 2023): 137.

Following a regulation on digital data, the level of safeguard would align with the laws.

The main concern at risk in regards to digital data are data breaches. When an organization or a state has a strong sense of network security and an effective incident response plan, it is better able to prevent cyber-attacks. 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. Hence, it is of great importance that the State must implement laws and regulations to protect the data of its nationals.

B. General Review on Trade

1. Review on The Basics of Traditional and Digital Trade

In the general definition, trade refers to the exchange of goods and services between one entity to another. Trade has been one of the most common forms of exchange since the beginning of mankind. The inability of a person to produce all of its basic needs triggers the need and importance of trade. Trade helps people exchange goods for other goods that it may not have. Hence, the concept of trade was created. Today, trade is conducted between States to exchange its goods and services.[30]

The classification of trade is further divided into 3 types: import trade, export trade, and entrepot trade. First, import trade, is the purchased of goods from a foreign State. State generally imports goods that are not produced

[30] Serlika Aprita dan Rio Adhitya, Hukum Perdagangan Internasional, (Depok: Rajawali Pers, 2020), 25.

domestically due to the inability to produce such goods for various reasons. Therefore, to meet to fulfil the needs of such goods, States conduct purchases from other States. Second, export trade would be the opposite of import trade. Export trade refers to the sale of goods towards a foreign State, it is the act of providing goods that are then purchased by other States. In this trade, goods are sent out towards other States. Lastly, entrepot trade is a combination of both import and export trade. It is the receival of imported goods which will be exported to another country. The goods are imported for the sole purpose of re-exporting to a third State.[31]

In the digital world, specifically in the telecommunication field, digitalisation enables a scale of trade in services that would have been unimaginable in an analogue world. Digital trade is now replacing major communication network as a result of the existence of internet and the web. Further resulting in new products, such as cloud services, whilst also having a significant transformative impact on many industries. In its aftermath, digital trade creates an effective economy that are supported by data applications.[32]

Today, trade has expanded to be an act conducted by States in cooperating to fulfil the basic needs of the people. Trade continues to expand to international trade and most recently within digital trade. The majority of

[31] Radius Logistics, What are the 3 types of international trade, https://radiuslogistics.co.uk/what-are-the-3-types-of-international-trade/

[32] Peter F. Cowhey and Jonathan D. Aronson, "A handbook of international trade in services," *Oxford University Press*, 401.

regulations on trade is under the World Trade Organization (WTO) treaties and agreements.

2. Review on International Trade Regulation and Its Application Within Digital Trade

International trade, understood as States cooperation through trade with one another to fulfil the basic needs of the people in accordance with their resources. It is the exchange of capital, goods, and services across nations and territories. The term international trade refers to the exchange of goods and services between nations, cross-borders. It contributes vastly in the increase of the world's economy. As States heavily rely on other States to fulfil the need for certain goods and services that is not provided locally. Traded goods and services ranges from raw materials, machinery, or food, and even extends towards a variety type of services.[33]

Throughout the years, international trade has increased exponentially and ranging in a variety of fields. Along with trade, follows an increase in private entities involvement in the production of goods and services among different countries. Private entities and production of goods and services hold a pivotal role in the expansion of companies to reach a larger group of people.[34]

---

[33] Aam Slamet Rusyadiana, "Perdagangna internasional," *Sekolah Tinggi Ekonomi Islam*, 2.

[34] Tatjana Boskov and Spire Lazaroski, *Globalization, Trade and Business*, 9 december 2011, https://core.ac.uk/display/35331351?utm_source=pdf&utm_medium=banner&utm_campaign=pdf-decoration-v1

As trade is cooperation between States, in conducting such arrangements, States create agreements between each other. For example, as practiced in the international community, there are a variety of trade agreements, as seen in the five major trade agreements, which include: the North American Free Trade Agreement, Central American-Dominican Republic Free Trade Agreement, the European Union, Arab Cooperation Council, and Regional Comprehensive Economic Partnership. These agreements act as a reference for the signing States in conducting trade with each other.

As time progresses, goods and services traded between State has shifted along with technological advancement and the expansion of communication network. With this new wave of goods and services, new agreements are created, as seen in the European commission on digital trade agreements, or Singapore's Digital Economy Agreements. These agreements are created to further regulate and accommodate the ever-growing new market of goods and services.

Despite the growing concerns and agreements on trade, international trade regulations have fallen behind in keeping up with the new wave of goods and services. In terms of international trade regulation, the WTO is still the main body that regulates on international trade. As its sole purpose, the WTO was created for the purpose of dealing with the rules concerning trade among States. The WTO revolves around their agreements and treaties, negotiated and signed by the world's trading nations and ratified in

their parliaments. The goal is to help producers of goods and services, exporters, and importers to conduct their business.

Under the WTO, there are two main agreements, which include The General Agreement on Tariffs and Trade (GATT) which is the central WTO agreement covering goods trade, and how States must conduct trade that is just for all States and its internal market. Second, the General Agreement on Trade in Services (GATS) which is the WTO's agreement covering trade on services. The GATS encompasses a much greater extent of matters on trade in a much general sense. Both GATT and GATS regulates the legality on international trade, and the permissible requirements for trade barriers, essentially having the same objectives, which include to create a credible and reliable system of international trade, allowing fair and equitable treatment of all member States, triggering economic activity through a strict and rigid policy, and lastly to promote trade and the development through progressive liberalization.[35]

In terms of digital trade, the WTO has never specified if their agreements are applicable in the digital world. However, seeing the nature of the GATT, member State of the agreement have differing opinions due to the fact that the GATT specifically focuses on standalone products and actual physical products, it heavily relies on tangible objects that has a

[35] The General Agreement on Trade in Services (GATS): objectives, coverage and disciplines (WTO), https://www.wto.org/english/tratop_e/serv_e/gatsqa_e.htm, accessed on 25 January 2024.

physical form. This nature does not exist within digital trade.[36] However, the member States has a differing opinion in regards to the applicability of the GATS within digital trade, this is due to the fact that the GATS provides a different perspective on trade.

The GATS is much broader in comparison to the GATT, the GATS covers economic activities breaching digital trade. The GATS is flexible enough to recognise bundles of services interconnected to the extent they constitute a distinct integrated service. The instrument regulates trade in a more general category of services. Hence, from this understanding, digital trade is more compatible following the regulations under the GATS, despite the WTO rules and practice not specifically regulating on data flows.

3. Review on The Application of Trade Barriers in the GATS and Its Application Within Digital Trade

Within international trade, trade barriers are permissible as long as certain requirements has been fulfilled. Trade barrier are restrictions established by the government for international trade. It is established to create a balance within international trade and the domestic trade within a State. However, there has been a debate on the permissible nature of trade barriers, as some may view such acts to decrease the overall economic efficiency.

[36] Communication by the United States WT/GC/16, G/C/2, S/C/7, IP/C/16/, WT/COMTD/17, 12 February 1999 (WTO, Work Programme on Electronic Commerce) ["WT/GC/16, G/C/2, S/C/7, IP/C/16/, WT/COMTD/17"]

It must be taken into account, that trade barriers are established to create a balance in national security and market as well as the international market as a whole. As a sovereign nation, States has the ability to prioritize its interest and its people. The obligation to maintain the wellbeing of the State prevails over the well-being of other State. In practice, trade barrier is imposed for certain conditions, such as: Protecting domestic employment, protecting consumers, protecting small industries, national security, and lastly, on certain occasion for retaliation.

The GATS allows the application of trade barriers with strict requirements that must be fulfilled. A few of the requirements 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." This rule is a commitment that implies for member Stats to not operate discriminatorily for the purpose of benefiting domestic services and 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. This rule requires State to maintain its commitments for market access that has been established.

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."
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."

The aforementioned requirements regulate on the permissible limits of trade barriers. As explained before, though not explicitly specified, the GATS does encompass its regulation to include digital trade. Referring to Article I of the GATS, the members defined trade in services towards 4 modes of supply:

First, cross border services, which are services applied from one territory of a member state into another territory. For example, a software that is operating in one member State by a supplier is sending electronic data towards consumers in another member's State borders.

Second, consumption abroad, this includes the act of providing services from one State to a consumer in a different State. Further includes the movement of the property of consumers in other States. For example, A social media headquartered located in one State is controlling data within a server located in a different State, to provide services in a third State.

Third, commercial presence, any services provided by a professional institution from a member State's territory towards another. Includes any services provided by a company owned by a member State's nationals, establishing a branch in another State.

Fourth, the presence of natural persons, this includes services supplied by nationals of one member State's to the territory of another member State. This mode includes both independent service suppliers, and employees of the services supplier of another member State.[37]

The WTO has defined electronic commerce as the production, distribution, marketing, sale or delivery of goods and services by electronic means.[38] Given the rise of digital trade and the ever-growing market on the internet, the acknowledgement of such forms of trade by the WTO requires digital trade to be consistent with WTO agreements. The general nature of regulations within the GATS creates a flexibility in its application.[39] The set

[37] Aaditya Mattoo, *National treatment in the GATS: Corner-stone or Pandora's Box*, "WTO Staff Working Paper", (Geneva, 1997): 5, https://doi.org/10.30875/b1dde982-en, accessed on 7 February 2024.
[38] Annual Report 1998 (World Trade Organizations, 1998), 35.
[39] The General Agreement on Trade in Services (GATS): objectives, coverage and disciplines (WTO), https://www.wto.org/english/tratop_e/serv_e/gatsqa_e.htm, accessed on 25 January 2024.

of rules regulated within the GATS apply across the broad towards all measures that effects trade in services towards market access and national treatment.

Thus, trade barriers regulation within the GATS does extend towards digital trade barriers. The application of trade barriers in digital trade may differ in its form, however, the rules and principle still apply.

C. General Review on Data Localization

As a result of the elements that has been explained above, States has conducted measures to protect its digital trade within its State, both for economic and data protection concern – Data localization was formed. Data localization is a domestic law that governs how data is processed within the State. It refers to how a data is collected, stored, transferred, and its movement inside and outside of the country. Some data localization may also be an administrative legal requirement whether directly or indirectly to the stored, processed, exclusively or non-exclusively, within a specified jurisdiction.

The application of data localization is consistent with the concept of data sovereignty, governing data processing within a State, in accordance with the prescriptive and enforcement jurisdiction as well as which laws could be applicable to the data subjects. With its ties to data sovereignty, data localization laws restrict the cross-border transfer of data. States applies its laws towards its data as it is the data of its nationals or accessible data within the State.

Given the concern of State's to protect its data within its sovereignty whilst keeping its digital doors open for foreign State's to enter – keeping the

digital market open, problems may arise if conducted with no restraint. Therefore, data localization is a State's effort to protect its interest within digital trade. The interest in question being its citizen's data, accessibility of data within the State, and foreign companies operating within a State. These efforts, if conducted excessively, may amount to a trade barrier that is inconsistent with international law, in this case, the GATS.

There are two types of data localization recognized: (1) absolute data localization, and (2) relative data localization.

1. 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.
2. 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. Commonly implemented by states, as it allows cross-border transfer of data which helps entities to transfer data for specific purposes.

States has taken different approaches depending on the degree it wishes to have control over its data. Regardless of which approach its takes, the regulation on trade barriers under the GATS would still apply. Hence, the international community must put int consideration a state's interest to protect

data within its sovereignty and measures that may amount to an impermissible trade barrier.

1. Review on Data Localization Regulation Practiced by the International Community

Data localization is practiced differently by States. Not all State has a data localization law. However, States who does have data localization laws varies in its form and application. Nonetheless, Numerous experts and States are beginning to come forward on its concerns of data localization laws that hinders and creates difficulties for States who would like to expand its digital market towards countries who has data localization laws.

There are a variety of ways that States implement data localization law, which include

a. Turkey – On October 1, 2020, amendments to the regulation of Internet Broadcasts and Prevention of Crimes Committed through such Broadcasts were created, also known as the social media Law in in Turkey. The new 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.
b. Russia – In Russia, Federal Law No. 242-FZ is a law that aims to protect Russian citizen's data by keeping it inside of Russia's Borders.

Furthermore, the law further regulates that personal information can only be collected for specific purposes stated in advance. The collection of personal data must be stored in databases inside of Russie. Requiring all companies to have servers within Russia.

c. India – The key data localization laws in India are regulated within a variety of laws. 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.

d. 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.

State practices as explained above shows the variety of ways State's uses data localization. In fact, the laws are also named differently, depending on what it is used for. However, any act that regulates the processing of data within a State are considered as data localization laws, though not mentioned directly within the law. The broad ways State's regulates on data localization may directly and indirectly effect at a different degree on digital trade within the international community. Hence, there must be a law that regulates its legality.

2. Review on Data Localization Regulation in Indonesia

Indonesia has implemented data localization laws for a long time. However, it has changed its data localization laws to be more lenient in the last few years. The major changes in Indonesia's data localization laws were between Government Regulation No. 82 of 2012 on Electronic Systems and Transactions and Government Regulation No. 71 of 2019 on Electronic Systems and Transactions.

Government Regulation No. 82 of 2012 on Electronic Systems and Transactions provides a restrict regulation regarding data processing for both public and private operators. It was required that all operators for Public Services in Indonesia had to establish a data centre in Indonesia resulting in many private sector companies being subject to the requirement to place a data centre within Indonesia. The law referred to the social

network provider as electronic systems operators also known as ESO that provide “public services” must establish a local data centre. The Ministry of Communications and Informatics defined public services in a broad sense, such that it would cover all services offered to the public on the Internet. As a result, numerous private sector companies were subjected to the data localisation requirement. Including businesses that largely operate online were greatly affected as they are now required to have a server within Indonesia’s jurisdiction to store its data. As the law required all data to be stored, collected and processed within the Indonesian territory. Furthermore, companies were under a much stricter rule in its operation. As the Indonesian government had to have full access to ensure its all-operators consistent practice within Indonesia. Further, it also had a negative impact on the government’s effort in promoting foreign investment.

However, within Government Regulation No. 71 of 2019 on Electronic Systems and Transactions, Indonesia takes a more lenient approach, as only government owned data are obligated to be stored within Indonesian territory. Private operators can now choose whether to process or store their electronic systems and data within or outside of Indonesia’s jurisdiction. Regardless of the location, companies must 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.