Pasadilla, Gloria O.; Duval, Yann; Witada Anukoonwattaka

Working Paper

Next generation non-tariff measures: Emerging data policies and barriers to digital trade

ARTNeT Working Paper Series, No. 187

Provided in Cooperation with:
Asia-Pacific Research and Training Network on Trade (ARTNeT), Bangkok

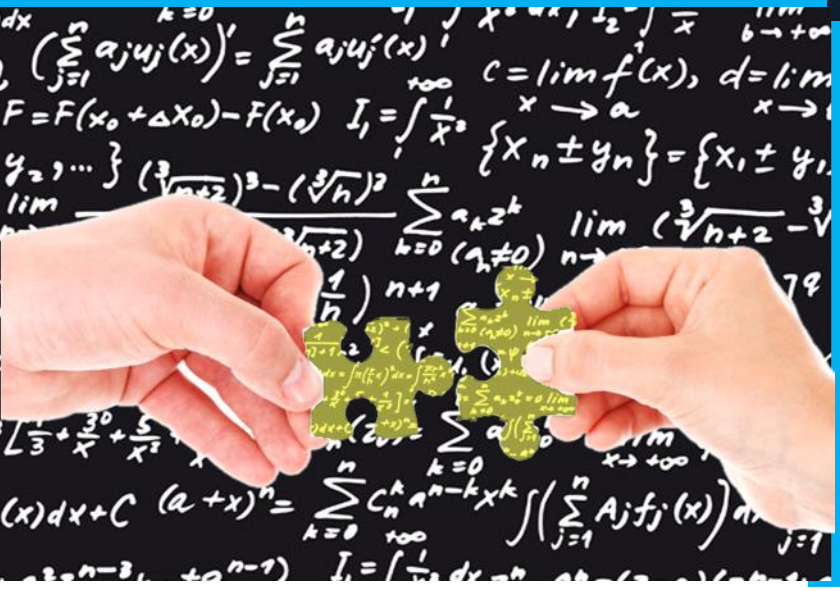
Suggested Citation: Pasadilla, Gloria O.; Duval, Yann; Witada Anukoonwattaka (2020) : Next generation non-tariff measures: Emerging data policies and barriers to digital trade, ARTNeT Working Paper Series, No. 187, Asia-Pacific Research and Training Network on Trade (ARTNeT), Bangkok

This Version is available at:
https://hdl.handle.net/10419/213424

ARTNeT

UNITED NATIONS ESCAP
Economic and Social Commission for Asia and the Pacific

Next generation non-tariff measures: Emerging data policies and barriers to digital trade



Gloria Pasadilla
Yann Duval
Witada Anukoonwattaka

ASIA-PACIFIC RESEARCH AND TRAINING NETWORK ON TRADE

Working Paper

NO. 187 | 2020

The Asia-Pacific Research and Training Network on Trade (ARTNeT) is an open regional network of research and academic institutions specializing in international trade policy and facilitation issues. ESCAP, WTO and UNCTAD, as key core network partners, and a number of bilateral development partners, provide substantive and/or financial support to the network. The Trade, Investment and Innovation Division of ESCAP, the regional branch of the United Nations for Asia and the Pacific, provides the Secretariat of the network and a direct regional link to trade policymakers and other international organizations.

The ARTNeT Working Paper Series disseminates the findings of work in progress to encourage the exchange of ideas about trade issues. An objective of the series is to publish the findings quickly, even if the presentations are less than fully polished. ARTNeT Working Papers are available online at www.artnetontrade.org. All material in the Working Papers may be freely quoted or reprinted, but acknowledgment is requested together with a copy of the publication containing the quotation or reprint. The use of the Working Papers for any commercial purpose, including resale, is prohibited.

Disclaimer:

The designations employed and the presentation of the material in this Working Paper do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. Where the designation “country or area” appears, it covers countries, territories, cities or areas. Bibliographical and other references have, wherever possible, been verified. The United Nations bears no responsibility for the availability or functioning of URLs. The views expressed in this publication are those of the author(s) and do not necessarily reflect the views of the United Nations. The opinions, figures and estimates set forth in this publication are the responsibility of the author(s), and should not necessarily be considered as reflecting the views or carrying the endorsement of the United Nations. Any errors are the responsibility of the author(s). The mention of firm names and commercial products does not imply the endorsement of the United Nations.

ASIA-PACIFIC RESEARCH AND TRAINING NETWORK ON TRADE

WORKING PAPER

Next generation non-tariff measures:

Emerging data policies and barriers to digital trade

Gloria O. Pasadilla, Yann Duval and Witada Anukoonwattaka

Please cite this paper as:

Pasadilla, Gloria, Duval, Yann and Anukoonwattaka, Witada (2020). “Next generation non-tariff measures: Emerging data policies and barriers to digital trade”, ARTNeT Working Paper Series No. 187, January 2020, Bangkok ESCAP.

Available at http://artnet.unescap.org

Abstract

Trade used to be about goods crossing borders and the instrument of protection was mostly through tariffs. Then there was greater recognition of trade in services, now exceeding the share of goods in global trade. Because of services, the focus of trade protection shifted more towards 'behind the border barriers' or domestic regulations that can obstruct services trade. More recently, the flows of goods and services are eclipsed yet again by data flows whose contribution to the economy is projected to reach 11 trillion USD by 2025. In the digital era, a new set of non-tariff measures – mostly related to data - have thus emerged. The paper seeks to understand the role of data in business and trade, the nature of some data flows restrictions and other digital trade barriers, and potential impact of data regulations.

Keywords: Data Regulations, Digital Trade, Digital Trade Barriers, Non-tariff measures, NTMs

Table of contents

List of figures

List of tables

1. Introduction

The face of global trade is evolving. Trade used to be about goods crossing borders and the instrument of protection was mostly through tariffs. Then, there was greater recognition of trade in services - either in itself or as part of manufacturing exports - now exceeding the share of goods in global trade. In services, the instrument used to protect domestic markets has shifted to regulations that can obstruct cross-border supply of services or the movement of capital and labor. More recently, the flows of goods and services are eclipsed yet again by data flows. While trade in goods, services and finance have grown 10 times larger since the 1980s until its peak in 2007, data flows (in terms of terabits per second) have increased 45 times in less than a decade since 2005. Data flows' contribution to the global economy was estimated at 2.8 trillion in 2014 and expected to grow to 11 trillion in 2025.[1]

Data also powers trade. Virtually every cross-border transaction uses data. From manufacturing to sales and post-sales, companies need and use data to support its activities and boost competitiveness. Data is also traded in themselves. Information generated through data analytics are valuable for marketing, for advertisers, for product introduction and design. Small wonder that the five biggest companies in the world today are in the technology sector which uses, processes, and generates huge data collected from all over the world.[2]

In the new era of trade, a new set of non-tariff measures - defined as anything other than tariffs that increase the cost of trade - are also rising. These new NTMs are policy measures that inhibit the cross-border transfer of data and consequently increase the cost of trading activities, much like the effect of traditional non-tariff measures on goods trade. These measures relate to data privacy and protection, cybersecurity and other digital trade policies. As with other non-tariff measures, these policies have positive effects on markets. Data protection policies help create trust, create markets, and increase the use of digital payments and purchases through e-commerce. Likewise, as with other NTMs, its application, details of implementations, and variable enforcements across jurisdictions are usually what create problems for businesses.

This paper attempts to understand the salient effects of this emerging 'next generation' of non-tariff measures. It starts with attempting to understand the role that data plays in business activities and trade and the potential impact of data regulations. Section 3 then discusses the

[1] McKinsey Global Institute. 2016. *Digital Globalization: the New Era of Global Flows.* March.

[2] These are Apple, Amazon, Alphabet (Google holding company), Microsoft, and Facebook (source: www.statista.com)

cross-border restrictions features of selected Asia Pacific countries' data privacy and cybersecurity laws, specifically data localisation and restrictions on data transfers. Section 4 deals with other digital trade barriers other than data policies, including digital taxation. Section 5 discusses the role of multilateral and regional trade rules in putting some disciplines in rules that restrict cross-border data flows. The last section concludes.

2. Importance of data in trade

The use of data is not only intrinsic to technology companies but is fundamental for businesses across sectors. Whether they operate only domestically or have export activities, the ability to move data is a central part of many business operations. Businesses collect customer information. If they have the capacity for big data analysis, they analyse customer data to tailor products and services better and to improve user experience. Doing these help them become more competitive and, often, lock in customer loyalty. Businesses need data for financial transactions. They also possess and use data of their employees, contractors and suppliers. In all its internal and external operations, they make use of data, personal data and otherwise.

For multinational companies, including manufacturing companies, that operate in various jurisdictions, data is needed to efficiently manage their supply chain. They share information on sales, inventories, shipping status and conditions, production schedules, and others. They use employee data to match skills within the organization and deploy manpower. To carry out research and development, they upload know-how, design or prototypes using cloud services - which imply data transfer - to facilitate the collaborative work among its in-house scientists and engineers and other external partners who may be working in different countries. In marketing and sales, data is critical to understand customer preferences and needs that, in turn, feedback into production and development of new products. Even post-sales, data is used for insight for generating new products or product improvements, research, as well as for repairs and maintenance of their equipment. Data moves in all directions all over the world and almost at every moment.[3]

[3] Kommerskollegium. 2014. "No Data, No Production". Sweden.

2.1 Reasons and nature of data regulation and why they impede trade

- **Reasons for regulations**

Countries adopt data policies that regulate flows of personal data in order to protect privacy. But different countries put different value to privacy which explains why privacy regulations differ across cultures.[4] Where privacy is considered a human right, privacy regulations tend to be more stringent. The presumption in some data flows restrictions with respect to data protection is that by locating data domestically, data would be better protected. This is not necessarily true however as data protection is also obtained with advanced technology and encryption. Putting data in defined servers may, in fact, attract more data hack and loss of data, while spreading them to unknown server location has a greater probability of data security (see Box 1). For example, it is alleged that storing data in just one location attracts hackers and makes data more vulnerable.

With respect to cross-border data flows, some countries regulate cross-border transfers of data for audit purposes. Governments want that they have ready access to information either for criminal investigation or regulatory/ supervisory purposes and this is, allegedly, facilitated if data is either stored and processed locally, or at least copies of it are kept within the territory. Another reason for regulation is industrial policy – with data considered as the new oil for 21st century trade, governments want to ensure that their industries benefit from the value that is generated out of their citizens' data and to boost local digital industries. Still another important reason for data flows restriction is national security, giving rise to data categorizations like 'important' or 'strategic' data (discussed in the next section) that are mandated to remain locally.

Box 1. How Google stores and moves data?

Google uses a distributed network to store and process data. What this means is that data is stored not in one server, or data center, or one location. Rather, data is usually duplicated, divided up into tiny packets, kept in multiple locations, and moved around in a 'smart' way. Arguably, doing so protects data. For example, problems in any one data center will not lead to loss of data nor make them inaccessible. Moreover, it allows users to access them easily, regardless of whether the user is in Asia or America. Routing data is likewise done to redistribute and balance the processing load and storage needs across different

[4] Lopez, J. and F. Casalini. 2018. "Trade and Cross-Border Data Flows". TAD/TC/WP(2018)19/Final. December Paris: OECD.

servers and data centers in different parts of the world. In the United States alone, Google operates at least 12 significant data centers, the largest known of them are in five different states. They also have data centers in Asia, Latin America, and Europe.

Source : https://www.blog.google/products/google-cloud/freedom-data-movement-cloud-era/

- **Personal data regulation is not as simple as it looks**

Personal and non-personal data are hard to separate

If data regulations restrict personal data, why would not businesses be able to operate 'normally' if they can transfer other types of data anyway? The thinking is that since know-hows, designs, production information, sensor information, and many others can be out of the regulatory net, businesses should be able to operate normally as long as personal data is protected, and better if stored locally. The problem with this assumption is that personal and non-personal data are difficult to disentangle. For example, in coordinating the various parts of a firm's value chain, personal data are used and generated (see Table 1)[5]. In designing new products, firms need data on how their customers use existing products; they also have the personal information of their scientists working in the laboratories. In post-sales, they use sensor data, but these usually come with the name of the employees or customers who operate the machine. To disentangle personal from non-personal data is a costly process.[6] The crux is that personal data is central to the production process even when apparently technical data is being shared cross-border. Hence, restrictions on cross-border personal data flows are almost the same as restrictions on all data flows (Kommerskollegium 2014).

Table 1: Personal data in the production process

	Personal data used	**Personal data generated**
Control/coordination	Employee data, user data, social media	Employee data
Pre-production	User data, social media data	Names and curriculum vitae of scientists/ researchers, test-persons' user data
Supply chain management	Customer data	Business contacts
Production	User data	Employee data

[5] Kommerskollegium. 2014. Ibid.
[6] Lopez, J. and F. Casalini. 2018. Ibid.

Post-sales	User data, sensor data	User data, social media data

Notes: User data refers to how a product is used. Employee data can include names, salaries, as well as how they operate a machine
Source: Kommerskollegium (2014), Table 2.

Vague definitions add to unpredictability

Besides being closely intertwined in the use and generation of production-related data, personal data and sensitive data are often vaguely defined in many privacy laws and this contributes to the difficulty of data transfers. In the first place, the definition of personal data is not uniform and well-defined. In many countries, personal data refers to anything that leads to an individual person being identified, which can include not only the usual information like address, birthdays, emails, etc. but also, in some instances, IP addresses. Moreover, many supposedly non-personal data can also lead to the identification of an individual if combined with other information. Thus, the potential scope of personal data becomes narrow or wide depending on how stringent the authorities' interpretation of the law is. Personal data definition's vagueness leads to business unpredictability.

Cybersecurity laws also tend to add to uncertainties about the data that can or cannot be transferred cross-border. For example, is machine prototypes (for new products) unequivocally considered non-sensitive information or is it considered 'strategic' data? In some countries, there are concerns that even intra-company transfers of product information can be looped into the net of data flows restrictions. Likewise, in countries where geographic mapping is barred, remote monitoring of equipment may not be possible unless stored in local data servers, limiting their use for analysis of product improvements. The wordings of some cybersecurity laws are equivocal about whether certain types of information are considered 'sensitive' or 'important' or 'strategic'.

2.2 Effects of data policies

With large penalties for non-compliance,[7] companies become very risk averse. Kommerskollegium's (2014) interviews of Swedish multinational companies show various responses. One response is to abandon the company's investment or expansion plans in jurisdictions where it is difficult to move data in and out of the country. Likewise, they also move out of countries where data protection is too lax that they risk being non-compliant with their own home countries' data protection policies. Another response is to decide to duplicate

[7]Penalties can be in terms of large fines (as in the European Union where fines can reach up to four percent of global turnover or 20 million euros, whichever is higher); or in terms of criminal liability and imprisonment.

their cost by building redundant data centers to comply with data localization or stringent data flows restrictions. This latter case is likely possible only for bigger markets but not for smaller economies.

Who get to participate in global value chains is also affected by data policies.[8] Companies have changed the configuration of their supply chain, switched suppliers and external partners from highly restrictive data flows countries with others from within the domestic or regional economy or from economies with similar data rules to its home economy or from jurisdictions where data flows are not restricted - even if they may not be the best ones. Working with SMEs has also become a problem if they cannot meet the high cost of data protection thus limiting SMEs access to GVCs.

The effects of data privacy laws and rules on cross-border data flows vary according to its stringency and the type of data that is required to be stored locally. If local storage applies only to a small category of data flows, e.g. financial data, its effects may be less compared to a vaguely worded law that can encompass almost all data flows. Similarly, the impact of cross-border data flows restrictions vary depending on whether copies are mandated to be locally stored or whether even data processing and use are prohibited to be done outside the country.

These different responses from companies possibly explain why recent empirical studies show that data policies adversely impact trade and productivity. Services sectors which are highly dependent on the internet and digital and data flows are negatively affected by data restrictiveness. Likewise, it has unfavourable impact on the performance of manufacturing firms that are highly 'servicified'.[9]

[8] Kommerskollegium. 2014. Ibid.

[9] See Ferracane, F and E. van der Marel. 2018. "Do data policy restrictions inhibit trade in services?" Digital Trade Estimates (DTE) Working Paper 02. Brussels: European Center for International Political Economy (ECIPE); and Ferracane, F., J. Kren, and E. van der Marel. 2018. "Do data policy restrictions impact the productivity performance of firms and industries?" Digital Trade Estimates (DTE) Working Paper 01. Brussels: European Center for International Political Economy (ECIPE).

3. Data protection policies in Asia Pacific

3.1 Cross-border data transfer policies in Southeast Asia, China, and other Asia Pacific countries

This section takes a look at cross-border data transfer policies in selected Asia Pacific economies.

- **Southeast Asia**

Southeast Asian countries have existing laws on data regulations, but while some have comprehensive data protection and privacy laws, others have data protection provisions spread out across a number of legislations. Where there is currently no comprehensive data privacy law (for example Thailand), a draft regulation is, nevertheless, under consideration. Cross-border transfer of data is generally permitted subject to data subjects' consent, and for as long as transferred personal data are accorded an equivalent level of security and protection in the recipient country or that organizations have taken all the necessary safeguards (including through specific contracts). Others put another condition that the data transfer is necessary for the performance of a contract between the parties (as in Malaysia). There are, however, cross-border transfer restrictions for data that are "material, strategic" (Thailand) or "state secrets" (Viet Nam) or "strategic" (Indonesia). Table 2 summarizes the salient features of data regulations in Southeast Asia.

There exist sectoral restrictions for cross-border transfer of financial and health information. For banks and regulated financial institutions (FIs), data flows restrictions are implied in central banks' regulations on outsourcing activities by banks and FIs because use of cloud services (which implies data transfers) is considered an outsourced activity. The requirements usually entail central bank's approval of the outsourcing activity by the bank and the data transfer if the cloud service is hosted offshore. This is the case, for example in the Philippines, Malaysia, Viet Nam and Thailand but not for Singapore where central bank approval is not necessary. However, central bank access to data for supervisory purposes or right to inspect the cloud facility is required in most outsourcing guidelines. Additionally, in the Philippines, a list of countries where data will be stored is required to be submitted to the central bank as part of the approval requirements.

Except for certain categories of data, localisation is not required in most countries. However, in Indonesia, the text of the current regulation requires electronic system operators that provide 'public service' (where 'public service' is very broadly defined) to have onshore data

centers to store and process data. The text is *prima facie* a data localisation policy but, fortunately due to strong business lobby, Indonesia is currently not imposing sanctions for non-compliance. A draft amendment to the data localisation law is under discussion where localisation is limited to 'strategic electronic data' but whose definition is still too broad. The draft amendment also restricts copies being stored offshore. In Viet Nam, data related to 'national security' has to be stored in onshore data centers. In addition, Viet Nam mandates the establishment of headquarters or representative offices in Viet Nam but further government guidance is being awaited to clarify whether the requirement applies to all organizations that provide services in cyberspace or own information systems in Viet Nam, or only to organizations that have very high number of users. The new Cybersecurity Law also needs further clarification on the scope of data to be stored, the organizations subject to it, and the duration for storing data.[10]

- **China**

China's data protection policies are contained in its consumer protection laws, cybersecurity laws and sector-specific laws (see Table 3).[11] The Cybersecurity Law which came into effect in June 2017 contains significant restrictions on cross-border data flows, along with technology regulation (requiring local certification or national security review) which businesses claim could exclude foreign products from the China market. It regulates critical information infrastructure operators (CIIO) and network operators (NO), both defined broadly and vaguely. CIIO are ultimately subject to the designation by the authorities and network operators in sectors like telecommunications, energy, transport, financial services and public services are likely defined as CIIO. There are also thresholds for being designated as CIIO such as the volume of users of the platform or their likely impact in case of a security breach[12]. On the other hand, network operator defined vaguely essentially includes any organization that operates a website or a computer network.

Personal data and 'important data' collected by CIIO are to be stored in China. 'Important data' is again vaguely defined as anything that has an important relation to national or security interest. These may be transferred cross-border if there is individual consent, if it is 'necessary' to send the data abroad and after a security review has been undertaken. The tests of 'necessity' and security assessment criteria remain unclear. Certain categories of data such as personal financial information and mapping data are to be localized.

[10] See Rajah and Tann Asia. 2018. "The Law on Cybersecurity". Client Update on Viet Nam.

[11] Information on China was drawn from Hogan Lovells, "Asia Pacific Data Protection and Cyber Security Guide 2018: Shifting Landscapes across the Asia-Pacific Region", downloadable from www.hoganlovells.com.

[12] Based on Cyberspace Administration of China (CAC)'s published 'Examination Guideline'.

The draft measure on security assessment of cross-border transfer of data extends the same obligation of CIIOs to NOs which will encompass almost all foreign corporations that operate in China. Even if the obligation for NOs (with lower threshold) end up being boiled down to only a self-assessment process of the necessity and security of their data exports, the compliance burden remains an issue of concern, particularly as it can change the condition of competition for foreign firms. Since foreign firms need to transfer data to parent firms abroad on an almost ongoing basis in the course of business, their compliance burdens can disadvantage them against their domestic competitors. Moreover, if the NOs reach a materiality threshold, self-assessment no longer suffices but an obligation to report the data export to authorities is triggered which could imply substantive review of each reported data transfer.

- **Comparison with other jurisdictions**

Although there are similarities in the data regulations among countries, the case of China stands in contrast with majority of countries. For example, the European Union's General Data Protection Regulation (GDPR)'s definition of personal data which encompass information relating to an identified or identifiable natural person is narrower compared to China's definition which includes 'activities' important to national security and social stability. Part of the reason for the divergence is that the Cybersecurity Law has a wider remit than specifically privacy protection. This also explains why, in addition, China empowers government authorities to inquire into the content of data and to establish additional categories of data that cannot be transferred. The EU, Japan and others, in contrast, require a designated government authority to oversee data privacy and enforce its data regulations but not inquire into the content of data to be transferred.

In general, Organisation for Economic Cooperation and Development (OECD) member economies like Japan, Republic of Korea, and Australia have more liberal policies with respect to cross-border data transfer if the recipient country has substantially similar data protection regime, adheres to similar privacy principles, safeguards are put in place for third party receivers of data (including through contracts), and individuals consent to the data transfer. There are some variations on data considered as sensitive that require more stringent regulations. For example, health records[13] in Australia have to be stored onshore, similarly with Republic of Korea. Japan appears to have a vaguer regulation in regard to patient data by requiring patient data be stored only in places where Japanese law is applicable. The

[13] Health records are sometimes part of employee data and hence relevant to the discussion here.

implication of this guideline from the Ministry of Internal Affairs and Communication appears to be a localization requirement.

In Japan, moving data to the cloud is not considered 'data transfer' but 'use' of data by the controller if control of the data remains with the controller and not with the cloud service provider (CSP).[14] The CSPs cannot use the data for any other purpose, let alone for advertising, than that necessary to provide the cloud service. Not being a 'transfer', putting data to the cloud thus requires no individual consent in Japan.

In India, data protection is included in the Information Technology Act of 2000 and Information Technology Rules (2011) but a comprehensive data protection law inspired by the GDPR is under discussion. The requirements for cross-border transfer of data are broadly similar to those of other countries such as, in the case of financial data, reporting requirement to the central bank or supervisory agency. The central bank has a 'white list' of pre-selected cloud service provider where banks can store their data. The requirement on safeguards, comparable data protection regime, individual consent, are roughly the same as in other jurisdictions (see Table 3). Interestingly, the draft bill of a comprehensive data protection law contains provision for localisation of all personal data, mandating that a copy be kept onshore and certain categories of personal data be classified as 'critical' and could only be processed in India. It remains to be seen how the final configuration of the Indian law with respect to cross-border data transfer and localisation would be.[15]

Box 2. Cross-border data transfer under EU's GDPR

The General Data Protection Regulation (GDPR) is touted as the most comprehensive, high standard data protection law with wide reaching implications for many companies in and outside of the EU. Its salient features include:

- Individual-centric provisions (mandating individual consent for the collection, storage, use, processing, transfer of personal data; right to be forgotten, data portability)
- Controller-processor model of data protection regulation with an independent data protection authority that can impose huge fines and penalties for non-compliance up to four percent of annual global turnover or 20 million euro (whichever is higher)
- Extra-territoriality of its applications

Data can be transferred outside the EU through various conditions: 1) through 'adequacy' finding of the rule of law (including privacy law) of the data recipient territory or sectors within a territory or international organization, that serve as guarantee for EU-equivalent level of

[14] Microsoft interactive guide for legal and compliance professional – Japan which can be found in www.microsoft.com website

[15] Global Data Review. 2018. "India's New Data Privacy Law- a Fourth Way". November

data protection; 2) through various safeguards such as binding corporate rules (BCRs), standard contractual clauses (SCCs), approved code of conduct, and certification mechanism; or 3) through various derogations such as consent by the data subject, necessity of transfer for the performance of a contract between data subject and controller, or for the purpose of a legitimate interest pursued by the controller which cannot be qualified as frequent and massive (Directive Article 7f and Regulation Article 49.1h).

Mattoo and Meltzer (2018) cites various limitations in the use of the derogations for cross-border data transfer. For example, transferring financial and personal information to complete an online purchase may qualify as 'necessary' but collecting other data incidental to the transactions such as consumer preferences would not muster the 'necessity' condition for the performance of the contract and unlikely to justify data transfer outside EU. The sufficient use of safeguards such as SCCs or BCRs is also in question before the European court of justice in Facebook versus Schrems case, in situations where the data receiving country has no comparable privacy regime that provides oversight and redress mechanisms.

BCRs refer to GDPR consistent corporate data protection policies which facilitate within-company transfers from the entity established in the EU to any of its subsidiaries, affiliates, or branches in the world. Standard contractual clauses (SCCs) which require the same levels of protection, oversight and access for individuals as would be the case within the EU also facilitate data transfer for companies established in the EU. Codes of conduct by associations representing controllers or processors, approved by the European Commission, and monitored and enforced within EU, is yet another way to show compliance with GDPR standards and thus allow cross-border data transfer. Finally, approved certification mechanism with their corresponding data protection seals and marks which shows GDPR compliance can be used by businesses outside EU as a basis for data transfer outside EU.

'Adequacy' finding refers to a decision by the European Commission that a non-EU country has an adequate level of personal data protection in view of its domestic law or international commitments. By far, 12 territories have been recognized as providing adequate protection, including New Zealand, Japan (most recently) and the United States of America (through the Privacy Shield framework agreement between the EU and the US). The effect of the adequacy decision is that personal data from the EU can flow to these territories without need for further safeguards (such as BCRs or SCCs and others).

Table 2: Data Protection Policies in Southeast Asian Countries

Country	Statutory Law	Cross-border data transfer	Data localisation
Indonesia	Government Regulation (GR) No. 82 (2012) on Electronic Systems and Transactions Sectoral laws exist	Permitted except for 'strategic data'. Finance – transfer is permitted for commercial banks but not for non-banking FIs, rural banks and guarantee agencies (data localisation). Data residency restrictions also apply to insurance companies. Health – covered by GR 82 and GR No. 46 which requires health information to be stored in Indonesian data centers linked with the database maintained by the Ministry of Health Registration requirement with Ministry of Communications and Information for electronic system operators	Onshore data centres and disaster recovery centres required for electronic system operators that provide a "public service"; 'public service' definition too broad – can cover all websites that collect and process information. Currently, there is no sanction for non- compliance Draft Amendment of GR 82 would clarify that entities are not prohibited from locating data centers outside Indonesia and that localisation is only required for 'strategic electronic data' (copies in overseas location not allowed). Strategic data defined as those with strategic impact on public interest, public service, smooth governance of the state or state defence and security. New data categories- introduced in draft amendment besides 'strategic electronic data'

Malaysia	Personal Data Protection Act (2010) regulates the collection, use and processing of personal data. Imposes similar obligations as in other countries on consent, transfers, and others. Personal Data Protection Act Standards (2015) confirm that there is no absolute requirement for data to reside in Malaysia Enforcing agency is the Personal Data Protection Commission.	Generally permitted. As long as requirement of PDPA are observed according to equivalent standards; data subject consent; transfer is necessary for the performance of a contract Finance –FIs' offshoring data requires approval from Bank Negara Malaysia (BNM). FIs are subject to banking secrecy obligations which prohibit them from disclosing customer account information. Approval requires BNM access Health – for private healthcare institutions – health and patient data must remain physically in the institution. No restrictions on other types of data. For public healthcare institutions – no restriction on use of public cloud services	No requirement for data to reside in Malaysia
Philippines	Data Privacy Act (2012) and DPA Implementing Rules and	Generally permitted.	None

	Regulations - regulate the collection, recording, organization, use and processing of personal data. DPA imposes obligations on notice, consent, purpose, disclosures, international transfers, security, data retention, data subjects' right of access and correction, and subcontracting. Enforcing agency is the National Privacy Commission	Finance – prior approval by the central bank (specifically the Core Information Specialist Group) required for outsourcing financial services. Outsourcing contract should include provisions to allow BSP to inspect operations of cloud services provider. FIs must submit to the central bank a list of territories where data will be stored.	
Singapore	Personal Data Protection Act (2014)- regulates the collection, use, processing of personal data; obligations on notice, consent, purpose, disclosures, international transfers, security, data retention, data subjects' rights of access and correction and subcontracting. Enforcing agency: Personal Data Protection Commission (PDPC)	Permitted. Requires organizations to put data safeguards (including contractual measures) to ensure that data transferred abroad is accorded comparable standard of protection under the PDPA. Anonymized data is not considered personal data. Finance - no government approval is necessary for data transfer but FIs must comply with MAS Outsourcing and Technology Guidelines. Ensures MAS	None

		has access to information for supervisory purposes Provides multi-tier certification for cloud services to provide transparency around the security service levels of cloud providers	
Thailand	Thai constitution recognizes and protects privacy rights of individuals but currently no comprehensive law on data protection. Draft Law is under discussion.	Generally permitted except for "material, strategic" services activities which require government approval to use offshore data centers (especially applies to regulated entities by Bank of Thailand (BOT)). Approval requires BOT access to information for supervisory purposes.	None. Draft law requires overseas data controllers to appoint a local representative and comply with the domestic privacy law
Viet Nam	New Law on Cybersecurity – covers network of IT infrastructure, telecommunication networks, internet networks, computer systems, information and processing and control systems and databases. Privacy requirements are spread across a number of laws such as Law on Cyber Information Security (Law No. 86/2015/QH13); Law on Protection of Consumers' Rights (Law No. 59/2010/QH12); Law on	Permitted except for information considered as "State Secrets" Finance – approval is needed for public financial institution to use cloud services; none for private banks; Health – public healthcare institutions need approval for use of cloud services. Definition of "state secrets" may include	Requirement to store within the territory data related to national security Requirement for foreign organizations to have HQ or representative office in Viet Nam (uncertain whether this applies to all organizations that provide services in cyberspace or owning information systems in Viet Nam or only to those with very high volume of users, e.g.

	Information Technology (Law No. 67/2006/QH11);	certain categories of healthcare information Data subject consent required for health data transfer	with more than 1 million users per month). Government guidance is awaited on establishment rules as well as on the scope of data to be stored, subject organisation, and duration for storing data

Notes: MAS= Monetary Authority of Singapore; BSP= Bangko Sentral ng Pilipinas; FI = financial institutions
Sources: www.microsoft.com/en-sg/apac/trustedcloud/ (Accessed 15 February 2019); lawgazette.com.sg (Accessed 23 February 2019); Rajah and Tann, Vietnam Law on Cybersecurity (Accessed 20 February 2019).

Table 3: Data Protection Policies in Selected Asia Pacific Countries

Country	**Statutory Law**	**Cross-border transfer of data**	**Data Localisation**
Australia	Privacy Act 1988 includes 13 Australian Privacy Principles Enforcing agency: Office of the Australian Information Commissioner	Permitted. Finance – notification with Australian Prudential Regulatory Authority (APRA) is required for cloud services considered as 'material outsourcing' by FIs; consult with APRA if services are provided outside Australia. Transfer permission premised on individual consent; service provider can give substantially similar data protection to those in Australia; service provider agrees to	Information contained in 'My Health Records' (a secure online summary of a patient's health information held by the Secretary of the Department of Health) cannot be stored, processed or handled outside Australia, but can be accessed by the individual even if he/she is outside Australia.

		contractual terms in line with the Australian privacy principles. Health – Public healthcare institutions are subject to their own respective State laws and regulations affecting health data. Cross-border transfer to a third party is permitted subject to any of the following requirements: 1) data destination jurisdiction has substantially similar privacy laws to Australia (or relevant State); 2) patient has consented and acknowledged that data held overseas will not be subject to Australian law; 3) the recipient agrees to be bound by Australia Privacy Laws in respect of that information.	
China	Cybersecurity Law (took effect in 2017) imposes obligations to network operators, especially to critical information infrastructure operators (CIIO). Enforcement is by Ministry of Public Security	Permitted for non-CIIO operators subject to individual consent and the entity initiating the data transfer the data had undergone a security assessment regarding its data transfers.	Under Cybersecurity Law, personal data and 'important information' collected in China must be stored in China (for critical information infrastructure operators CIIO). Definition of CIIO depends on the industry and how much data breach would harm the public interest. Likely

	(especially Cyberspace Administration of China (CAC)) Draft Measures for Security Assessment of Cross-border Transfer of Personal Information and Important Data (Security Assessment Measure) – expands scope of data to include person's activities and behaviours Draft Guidelines for Data Cross-Border Tansfer Security Assessment (Guidelines) – List types of 'important data' The two draft measures apply to 'network operators' engaged in domestic operation. Network operator include any person or entity that owns and manages any network and also network service providers. Domestic operation means providing products and services within China	Personal data and 'important data' collected by CIIO may be transferred overseas but requires prior regulatory approval after filing the security assessment report with the designated authority. Data export only allowed if the authority agrees that it is genuinely necessary for business reasons to transfer the data Draft Guidelines and Measure require network operators engaged in domestic operation to conduct security assessment (an internal self-certification process) before engaging in cross-border transfer of personal information and important data. Rules do not apply to network operator located in China that provides only products and services to foreign entities and whose operation does not involve any personal information of Chinese citizens or important data. Draft Security Assessment Measure require consent of data subject for the overseas transfer and notify them of: 1) type of data being transferred; 2) purpose and scope of the transfer; 3) recipient and the country to	CIIOs are network operators in public communication and information service, energy, finance, public services. Financial personal data of Chinese citizens collected in China should be stored, processed and analysed in China. It cannot be transferred without approval from the People's Bank of China (PBoC). Branches of foreign banks may transfer, process, and analyse data to their parent banks if certain criteria are satisfied. Health data – to be stored in China

		which data will be transferred. Consent may also be implied in some cases Data captured from Chinese citizens visiting foreign websites are not considered data transfer (carved out), but data storage in clouds in offshore data center even if fully encrypted and controlled by Chinese data controller constitutes a transfer	
Japan	Personal Information Protection Act (2003) (PIPA) regulates the collection, use and processing of personal data. Enforcing agency: Personal Information Protection Commission (PICP) – has jurisdiction over all matters relating to personal information.	Permitted with the right safeguards in place. Cloud data storage is not considered data transfer under PIPA under certain conditions: 1) cloud service provider has no authority to handle data stored in its data center; 2) required to establish a proper access control system under its service agreement with the customer. Thus, data storage in the cloud may not require individual consent. Cloud service provider should not use healthcare institution's data for any purpose other than that which is necessary for the cloud service. For example, it cannot use it for advertising	Health – patient data to be stored in a place where Japanese law is applicable. Implication of this guideline from the Ministry of Internal Affairs and Communication is unclear as to whether offshoring of patient data is prohibited.

India	Information Technology Act (2000) and related rules provide for the protection of data stored on computer, computer systems, networks and computer resources. Information Technology (Reasonable Security Practices and Sensitive Personal Data or Information) Rules (2011) regulate the collection, use and processing of personal data Ministry of Electronics and Information Technology (MeITY) oversees the enforcement of the privacy rules. A draft bill of a comprehensive data protection law is under consideration	Permitted. Finance – requirement to report to Reserve Bank of India (RBI) the scale and nature of outsourced activities, geographic locations where data and operations are stored/processed abroad. Can transfer to pre-selected (empanelled) cloud service providers. Public sector banks require permission to transfer data outside India. Insurance companies must report to its own regulatory agency. Health – cross-border transfer of sensitive personal data is permitted, provided healthcare institution take appropriate safeguards (including contractual measures) to provide comparable data protection required the Indian Privacy Rules, patients' consent is obtained or the transfer is necessary for the fulfilment of lawful contract between healthcare institute and patient.	Insurance companies have data residency requirements for: investment data, accounting systems, core life policy administration systems, channel management systems and financial systems (need to be stored in onshore data centers) Draft bill under consideration contains provision for data localization of all personal data – one copy to be stored onshore. The government may classify certain categories of personal data as 'critical' data that can only be processed in India.
Republic of Korea	Act on Promotion of Information and Communication Network Utilization and Information	Permits transfers in the context of outsourcing (with written outsourcing agreement and notification/disclosure of	UPC cannot leave Republic of Korea and cannot be processed through the cloud unless reclassified as non-

	Protection (Network Act) and the Personal Information Protection Act (PIPA) – regulate the collection, use and processing of personal data Act on the Protection, Use, etc of Location Information (Location Information Act) – regulates collection, use and processing of personal location information Enforcing Agency for PIPA: Ministry of Interior and Safety For Network Act and Location Information Act: Republic of Korea Communications Commission has jurisdiction Republic of Korea Internet and Security Agency – for monitoring compliance with personal data protection laws	outsourcing arrangement). Network Act requires individual consent except if the transfer is necessary to perform its contractual obligations and enhance user's benefits; data transfer is disclosed in the privacy policy; safeguards are in place to protect personal information Finance – non-critical information or de-identified critical information such as Unique Personal Info (UPC) (eg. National Registration Number, passport number, driver's license, foreigner registration number) or Personal Credit Information can be transferred but should be reported to the Financial Supervisory Commission (FSC) Health – Not permitted for electronic medical records	critical (ie. If de-identified or not related to electronic financial transactions (eg HR systems or group-wares including mail system) Electronic medical records must be stored in Republic of Korea, not in offshore data centers

Sources: www.microsoft.com/en-sg/apac/trustedcloud/; Hogan Lovells. 2018. "Asia Pacific Data Protection and Cyber Security Guide 2018: Shifting Landscapes across the Asia-Pacific Region", downloadable from www.hoganlovells.com.

4. Beyond Data Regulations: Other Barriers to Digital Trade

This section briefly touches upon other barriers to digital trade beyond data regulations. Each of these other barriers deserves more in-depth discussions but for the purpose of the paper, the section only highlights a few of the issues.

- **Digital Taxation**

Besides data regulations and policies, other barriers to digital trade are emerging. Perhaps the one that is rapidly being rolled out in several countries is digital taxation. Under current tax laws of most countries, services provided online by foreign providers are not taxed in the country where the service is consumed but are taxed in the countries where the service provider is established. But with ballooning consumption of foreign online services, governments are bemoaning large revenue losses from untaxed online consumption. Local services providers also feel that they are disadvantaged because while they have to pay local VATs, their foreign online competitors do not. To level the playing field, several countries have started to adopt digital taxes.

How these are implemented raise interesting issues. In EU for example, the French-led digital tax proposal of imposing a tax of three percent of turnover from certain digital services, specifically sale of online advertising space, fell through because of, among other issues, perceived targeting of big American technology firms.[16] In Singapore and in other economies, online registration of foreign online businesses exceeding a certain threshold of domestic turnover will become mandatory for tax payment purposes in 2020 notwithstanding that the entity has no local presence or establishment. Other countries like Australia, India, Japan, New Zealand and Republic of Korea, have also promulgated rules requiring online suppliers who sell in their domestic markets to register for VAT. More will likely follow. Most digital tax systems rely on self-reporting by foreign online businesses and tend to target those with high online customer base or turnover.

Still another form of digital taxation is the so-called 'Netflix' tax by requiring a contribution to subsidize the local film industry (for example, in France or Brazil) or to compensate cable service providers (for example, in Argentina).[17]

[16] France decided to go it alone after the EU members failed to agree on an EU-wide digital tax policy.
[17] Ferracane, M., H. Lee-Makiyama, and E. van der Marel. 2018. *Digital Trade Restrictiveness Index.* Brussels: European Center for International Political Economy (ECIPE).

The problem at issue is that tax rules have always been based on the principle of 'establishment' or physical presence. Developed for brick and mortar companies, tax rules seem not adequate for online businesses. The argument for 'fairness' of digital taxation is that countries where online users of a service are significant contribute to value generation because users' data add value. Hence these countries should legitimately get its share through taxation of foreign businesses that have no physical presence in the taxing jurisdiction. The question is where real value in fact resides. It is deemed that value is derived from knowledge and innovation, from algorithms, softwares, and analysis, and yes, also from user data.[18] But user data contribution may or may not take place depending on the type of digital service.

Another issue is the risk of double or multiple taxation. Current bilateral tax treaties may not allow for deduction of digital service tax in the computation of tax liabilities in the home jurisdiction. That tax is slapped on turnover instead of profit is another issue of (un)fairness because some businesses may have high turnover but low margins while others have high margins and low turnover. With turnover taxation, even start-ups that are typically still operating at a loss are taxed. Compliance burden is another issue that can saddle SMEs that get caught in the digital tax net especially with regard to reverse charges. In Singapore, import of online services will start being accounted for, including by previously exempt GST taxpayers.[19] This could lead to escalating compliance cost that can especially burden SMEs.

- **Technology Standards, Filtering and Other Barriers**

Technology standard is another battleground in digital trade. For example, China's WAPI (WLAN Authentication and Privacy Infrastructure) is feared to fracture the WLAN (wireless local area network) equipment market because WAPI differs from the global standard. The International Organization for Standardization (ISO) rejected the WAPI and instead supported ISO 802.11i security specification that was developed by the Institute of Electrical and Electronic Engineers (IEEE). However, in China, foreign companies cannot have the foreign technology certified, albeit based on global standards, and are forced to establish separate operating platforms for the China market. The different standards lead to technology fragmentation.[20]

Moreover, the details of the WAPI standard which is in use in government agencies are known to only a few Chinese equipment makers. This makes it difficult for foreign technology suppliers to

[18] https://home.kpmg/be/en/home/insights/2018/08/fair-taxation-of-the-digital-economy.html

[19] Ernst and Young. 2018. "Rising to Digital Taxation". *You and the Taxman,* Issue 1.

[20] In some way, this had always been true with issues of standards. Many countries insist on their domestic standards despite the fact that adopting international standards facilitate exchange. For example, it took years before the UN/EDIFACT (UN Electronic Data Interchange for Administration, Commerce, and Transport), a set of syntax rules for data structure, was approved as ISO standard 9735.

bid in government procured projects. Consequently, either they license their technology to Chinese vendors or, if they fear leakage of their intellectual property, are forced to stay out of the Chinese market. Another issue related to government technology procurement is the mandated surrender of patents and source codes as a requirement for participation.[21]

In some cybersecurity laws, telecommunication companies and internet service providers (ISPs) are obliged to monitor content and ensure network security. They are required to take down contents that are 'objectionable', usually relating to extremism or terrorism. The difficulty is that different countries may have different thresholds for 'extremism' that can range from criticism of the government (which is acceptable in most democratic societies while not welcome in others) to genuine terroristic activities.

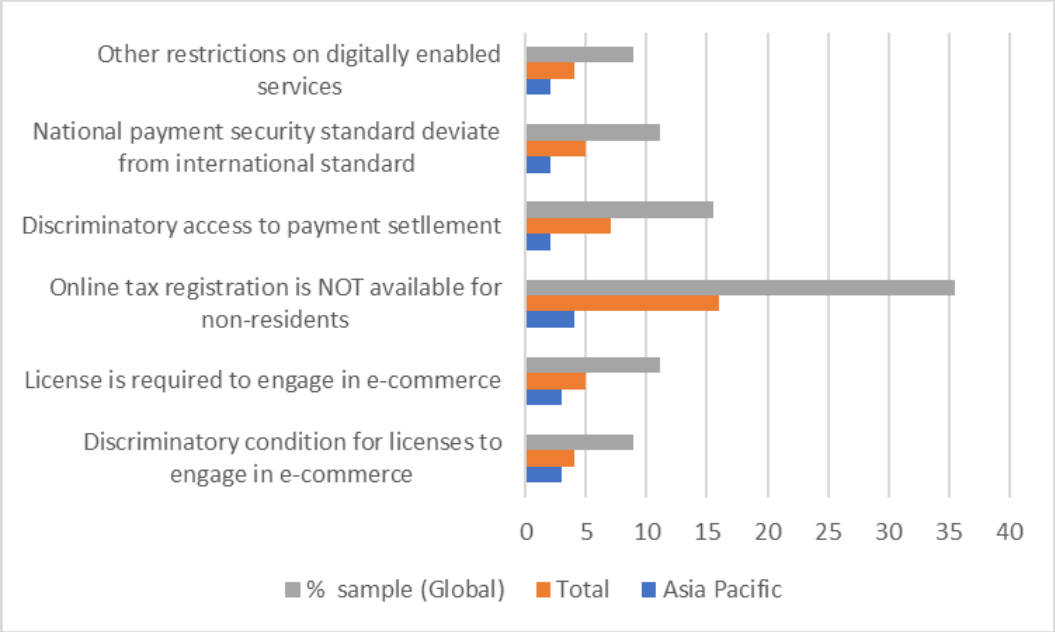
Content blocking, filtering and geo-blocking are other obstacles to digital trade. For example, e-commerce sites from certain jurisdictions may not be viewed in another country and are thus unable to sell products there via e-commerce. Yet, the blocking country's e-commerce sites can be accessed in this other jurisdiction and can sell products unhampered.

Employment laws for IT professionals are also protective of local citizens. In Indonesia, for example, electronic service providers are required to hire Indonesian citizens to operate 'strategic' electronic systems.[22]

Sectoral restrictions also affect digital trade. In financial services, access to national payment settlement systems may be discriminatory. Commercial presence may be required to provide cross-border services. There may be restrictions on online advertising or limitations on downloading or streaming content. A selection of some of these measures and the number of countries which have them are shown in Figure 1.

[21] Ferracane, et.al. 2018. ibid
[22] Ferracane, et.al. 2018. Ibid.

Figure 1: Selected measures that affect digital services trade (number of countries)



Source: Author based on OECD DSTRI data base. Number refers to the number of countries in the OECD sample

5. Data regulations and trade rules

Given the increasing number of data regulations and other digital trade barriers that impact global trade, a question that is asked is whether existing multilateral or regional trade agreements have the rules that can apply to new non-tariff measures like data localisation. The question is salient because existing multilateral trade rules were agreed mostly in the pre-internet era when many digital applications were not in commercial existence and their impacts yet unknown. Google and Facebook, for example, were not yet then a household term, yet they loom large in today's trade discussions. More recent preferential trade agreements have sought to remedy the apparently missing elements in multilateral rules by incorporating chapters on e-commerce and regulations on cross-border data flows and data localization. The section looks briefly at the WTO agreement provisions that relate to digital trade as well as the data flows provisions in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), US-Mexico-Canada Agreement (USMCA) and EU-Japan trade agreement.

- **WTO and the digital economy**

Trade rules bear on digital trade in at least three ways[23]: 1) through rules that regulate trade in goods and services; 2) through rules beyond-the border that demand changes in domestic regulation; and 3) through the limits on the policy space of regulators.

With respect to trade in goods, the World Trade Organization (WTO) had a liberalizing effect on digital economy through trade liberalization of technology products, disciplines on intellectual property rights (IPR) protection, and behind-the-border regulations affecting product standards as well as services. The information technology infrastructure supporting the internet is an important precondition for connectivity and access to digital applications. In this regard, liberalization of trade in technology products through, for example, the Information Technology Agreement (ITA) supported the growth of the digital economy. The technical barriers to trade (TBT) agreement also provides discipline through non-discriminatory norms and procedural safeguards aimed to encourage subscription to international standards and to discourage use of domestic standards as a barrier to trade. Whether the TBT agreement has relevance to the current debate on wireless internet standards that is feared to balkanize the internet remains to be seen.

With respect to services trade which, unlike goods, cannot be stopped at the border, sectoral commitments on domestic measures and classification categories hold the key for whether the services agreement is relevant to digital trade issues or not (see Box 3 for financial services).[24] A major limitation of the W/120 services classification that was used for the GATS negotiation is that many internet-related services were non-existent then and thus currently hard to pigeonhole in the W/120 categories. For example, online games as a new type of content platform could be categorized under computer and related services, value-added telecommunications services, entertainment, or audio-visual services, each of which implies different set of duties and/or flexibilities, depending on whether the country has committed the sector and the details of its commitments.[25] Consequently, data flows connected with online games may or may not have protection under the GATS. Discussions at the WTO on whether electronic data flows should have a separate classification, i.e. distinct from goods or services, or should continue to be discussed under services, are ongoing.

[23] Burri, M. 2017. "The Governance of Data and Data Flows in Trade Agreements: the Pitfalls of Legal Adaptation." *Law Review*. Vol 51:65. University of California- Davis.
[24] The General Agreement on Trade in Services (GATS) has most-favoured-nation (MFN) as a core general obligation, supplemented by countries' sectoral commitments on market access and national treatment.
[25] Burri, M. 2017. Ibid.

General Exceptions chapters put additional flexibilities in GATS as well as in GATT. GATS exemptions (Article XIV) may be invoked for measures that violate a country's obligations and commitments but justified in the pursuit of legitimate public policy objectives. Two such objectives are relevant for data flows: 1) those relating to public order or public morals; and 2) those that countries consider necessary for national security. Use of general exceptions, however, is so circumscribed by the 'necessity' test used in WTO dispute settlement decisions. For example, invoking national security exception is limited to: 1) provisioning the military; 2) activities related to fissionable and fusionable materials; and 3) measures taken in times of war or other international emergencies. In theory, these are hard conditions to satisfy if countries want to use security exceptions as defense for their stringent cybersecurity laws restricting data flows.[26] By far, the success rate among dispute settlement cases in the WTO for passing the 'necessity' test in invoking the general exception has been low.[27]

Box 3. Data flows, payments services, and WTO rules

The relevant GATS commitments and obligations that bear upon data transfer or data localization in financial services are:

a) National treatment obligation (if there is commitment in the sector) may be violated if there is local processing and storage requirement as this potentially changes the condition of competition between foreign and local service suppliers.
b) Annex on financial services: ban on cross-border electronic transmission of data that constitutes the service may be inconsistent with relevant market access commitments (if a Member has committed the service sector).
c) Annex on telecommunications: ensures that foreign service suppliers are allowed to use basic telecommunications for the movement of digitized information within and across borders including for intra-corporate communications. The Annex recognizes information flows as essential to transmitting services and a means of conducting business operations.
d) Understanding on commitments in financial services: constitutes a pledge not to take measures that prevent transfers of information or processing of financial information, including transfers of data by electronic means while recognizing the right of Parties to adopt measures to protect personal data, personal privacy, and confidentiality.

Source: Author's regional trade policy course lecture notes.

[26] https://www.lawfareblog.com/us-criticism-chinas-cybersecurity-law-and-nexus-data-privacy-and-trade-law
[27] Burri, M. 2017. Ibid.

Preferential Trade Agreements

- **CPTPP**

The CPTPP was signed by 11 Asia-Pacific economies in 2018. Besides being a large regional grouping that comprises 14 percent of the global economy, the CPTPP is tauted as a next-generation type of trading agreement, particularly as it addresses many technology barriers.

Unlike the WTO which has sectoral or indirect provisions on data flows (see Box 3 above), the CPTPP has a specific chapter on e-commerce which includes, among others, cross-border data flow provisions and prohibition of data localization. Article 14.11.2 states that "*Parties 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*". Moreover, Article 14.13 expressly prohibits data localisation as a condition for conducting business in the territory – unless it is to achieve a "legitimate policy objective (Article 14.13.3)". However, 'covered persons' as defined in the chapter does not include 'financial institutions' and cross-border 'financial service suppliers' – the so-called financial services carve-out under the CPTPP.

The financial services chapter, however, contains obligation to allow financial institutions to transfer cross-border information in electronic or other form, including for data processing if such processing is required in the ordinary course of business. However, unlike the e-commerce chapter, the CPTPP's financial services chapter does not include prohibition of local data storage or local processing requirement. Based on prudential considerations, authorization or approval by relevant authorities may also be required prior to data transfer to designated recipients (see Table 3 above). However, there is uncertainty on what constitutes a 'financial institution'. In some jurisdictions, e-payment service suppliers would not qualify as a financial institution under the CPTPP definition of a financial institution because they are not supervised as such.[28] In contrast to the CPTPP, the GATS Annex refers to financial services supplier which is more general than the term financial institution and can thus include e-payment service providers.

- **USMCA and EU-Japan**

The USMCA is the updated version of North Atlantic FTA signed in 1993. Like the CPTPP, it contains provisions on cross-border data transfer but with a noteworthy stronger language. In the

[28] CPTPP defines financial institution as "any financial intermediary or other enterprise that is authorised to do business and regulated or supervised as a financial institution under the law of the Party in whose territory it is located." This means that different jurisdictions may have different definition of financial institutions. In some countries, an e-payment service provider may not be supervised as an FI, hence some provisions in the financial services chapter may not apply to them. For example, Article 11.15 states that financial institutions (of other Parties) are accorded national treatment in accessing the national payment and settlement system (of another Party). Whether e-payment service provider would likewise be given national treatment is not explicit in Article 11.

CPTPP, the provision states “each party shall allow the cross-border transfer of information…”; in the USMCA, the wording goes: “no party shall prohibit or restrict the cross-border transfer of information…”. In addition, the prohibition on localization of computing facilities has less wiggle room in the USMCA, while the CPTPP allows room for exceptions for legitimate public policy objectives.

In contrast, the EU-Japan trade agreement has no provision on data flows except to state that the Parties will reassess within three years of the date of entry into force of the agreement whether such provisions should be included. Instead, almost immediately after the conclusion of the trade agreement, EU and Japan gave a mutual adequacy ruling on both their data regulations after Japan had agreed to make some additional changes in its privacy regulations which provide additional data protection as in the GDPR. The changes include individual right of access and rectification, transfer to third countries, and expansion of Japan’s definition of ‘sensitive’ data. Japan also gave assurances on data access by Japanese authorities for law enforcement and national security purposes by establishing a dispute resolution mechanism for complaints under the supervision of the Japanese data protection authority. Under the GDPR, an adequacy ruling by the EU means that transfers of European data to Japan will not need a specific authorization.

Meanwhile, the EU has released a recent proposal for horizontal provisions on cross-border flows and personal data protection which will presumably be used in future trade agreements prohibiting localization and regulating restrictions on cross-border data flows. It is essentially similar to the CPTPP provisions along with the regulatory space for data security and protection rules.[29]

6. Summary and Conclusion

The digital transformation of the economy and of global trade has brought opportunities and new challenges. It allowed new businesses to spring up, including from SMEs; connected billions of people to a wider world; created new efficiencies from production; and ushered many more benefits. But along with it came the loss of privacy and greater risk in security. The search for the proper balance is on.

The quest for a solution also affects trade. Some of the responses to the negative drawbacks from digitization give rise to a set of new measures that will increase the cost of trade. Since the

[29] http://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf

digital economy depends on data and its free flows, data regulations of countries, particularly those that restrict cross-border flows and the requirement to build computing equipment to store data locally, are an emerging kind of non-tariff measures that will need to be more closely examined.

There are various reasons for restrictions of cross-border data flows and localisation. These range from privacy protection to national security to industrial policy. Their immediate impact is heavier compliance burden, higher cost of business operation, and over the medium to long-term, multiplication of redundant data centers and loss of efficiency.

Asia Pacific economies are among those that have passed or are discussing comprehensive laws on data protection. Their stringency on cross-border data flows vary; some require localization of certain categories of data; and in some cases, even if cross-border flows are allowed, the vagueness of the legal text may effectively result in data localisation. In laws that are currently being considered, the influence of EU's GDPR especially its emphasis on individual right to privacy is discernible. While the GDPR does not expressly prohibit cross-border data flows, the compliance cost can become prohibitive for many small businesses.

Besides data policies, other barriers to digital trade include the rising number of digital taxation policies, technology fragmentation due to differing standards, geo-blocking, filtering, and many others that this paper does not discuss.[30]

Multilateral trade rules are said to already contain some disciplines on restrictions of cross-border data flows, particularly as they affect trade in goods and services. These disciplines, however, are circumscribed by general exceptions for legitimate public policy objectives. New preferential trade agreements such as the CPTPP and USMCA, however, have moved ahead with explicit legal text to facilitate e-commerce and digital trade which will likely influence further trade negotiations even at the multilateral level.

In summary, no country can join the digital economy transformation without data flows and right data policies. Whether regulators like it or not, digitization requires data to wander "almost everywhere and almost all the time". The challenge is data privacy and security which many technology businesses are addressing through advanced encryption technology and protocol. In fact, with greater popular awareness over data privacy, the capability to secure and protect data has become a competitive edge for big technology companies. This brings another type of challenge – that of competition policy – because the high cost of maintaining secured data

[30] For details of other digital trade barriers, see ECIPE's index of digital trade restrictiveness

centers, in terms of hiring and maintaining digital talent, building infrastructures –data centers that are spread out globally – and constantly upgrading technology, is a formidable entry barrier that leads to market concentration among few and large cloud services companies. As the digital economy continues to grow, enhanced regional and multilateral cooperation will be necessary on developing policies and regulations to address these issues in a way that does not create unnecessary barriers to trade and supports inclusive and sustainable development.

The Asia-Pacific Research and Training Network on Trade - ARTNeT - is an open network of research and academic institutions and think-tanks in the Asia-Pacific region. Since its inception, ARTNeT aims to increase the amount of high quality, topical and applied research in the region by harnessing existent research capacity and developing new capacities. ARTNeT also focuses on communicating these research outputs for policymaking in the region including through the ARTNeT Working Paper Series which provide new and policy–relevant research on topics related to trade, investment and development. The views expressed in this publication are those of the authors and do not necessarily reflect the views of the United Nations and ARTNeT secretariat or ARTNeT members.

This and other ARTNeT publications are available from **artnet.unescap.org**

ARTNeTontrade

@ARTNeTontrade

ARTNeT Group

artnetontrade@un.org

ARTNeT Secretariat, United Nations ESCAP

Rajadamnern Nok Avenue

Bangkok 10200, Thailand

Tel: +66(0) 22881410

Fax: +66(0) 22881027