International Journal of Business and Society, Vol. 21 S1, 2020, 66-80

INTERNATIONAL NORMS IN REGULATING E-COMMERCE: THE ELECTRONIC COMMERCE CHAPTER OF THE COMPREHENSIVE TRANS-PACIFIC PARTNERSHIP AGREEMENT

Ida Madieha Abdul Ghani Azmi[♣]
International Islamic University Malaysia

Jeong Chun Phuoc
Management and Science University

ABSTRACT

The Malaysian government has introduced a number of flagship initiatives to leverage on digital economy and tap the economic trade benefits it promises to the country. For digital economy to grow to its utmost potentials, a supportive eco-legal system is warranted, both at domestic level and international level. As at the heart of digital economy is speedy access to Internet as well as latest gadgets, applications and data analytics, facilitating transfer of data from one country to another should be a matter of first priority. Whilst government seeks to achieve that domestically by introducing relevant laws and regulations, it is no surprise that international norms on data transfer is equally imperative. Using doctrinal analysis, this article explores the provisions of the E-Commerce Chapter of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and compares them with existing domestic legal obligations. The E-Commerce chapter that contains provisions on spam, online personal data, location of computing facilities, among others, are in some ways requiring enhancement of existing legal obligation. The paper concludes that implementing CPTPP would not require much structural changes to the existing suite of e-commerce related legislation in Malaysia.

Keywords: Digital economy; E-commerce; CPTPP; Spam; Personal data protection; Online consumer rights; Forced local computing facilities and cross border data flow

Received: 11 February 2019
Accepted: 20 August 2019

1. INTRODUCTION

In 1993, the rock band, 'Cranberries' released "*Everybody Else Is Doing It, So Why Can't We?* (The Cranberries,1993) which took the world by storm. The vivacious verve in the album epitomizes the current spirit of the 21st century digital economy embraced by contemporaries (ALRC, 2018). The term 'digital economy' refers to an economy which functions primarily by means of digital technology, especially electronic transactions made using the Internet (Oxford

♣ Corresponding Author: Department of Civil Law, AIKOL, International Islamic University Malaysia, Kuala Lumpur, MalaysiaE-mail: imadieha@iium.edu.my

Dictionary, 2018). Coined by Don Tapscott (1995) in his book *The Digital Economy: Promise and Peril in the Age of Networked Intelligence*, it heralds a new economic future that will change human's lifestyle and ways of doing business. The 21st century digital economy is all about the Internet of Things (IoT) that drives digital convergence and digital entrepreneurship (OECD, 2018). Fintech, crypto-currency, block-chain technology and Sophia (AI-powered humanoid) are raved examples as challenges to legal regulation of the digital economy (OECD, 2018).

Malaysia, like the rest of the world, has embarked on national policy strategies and initiatives to develop its innovation led growth economy, and is putting a lot of emphasis on the digital economy (World Bank, 2018). In Malaysia, e-commerce is strong in terms of growth rate and commercial players. The World Bank Report projected e-commerce in Malaysia to exceed RM110 billion by 2020 (World Bank, 2018).

Around the globe, national countries are responding to notion of 'digital economy' in their national policies. The first report is the United Nations Conference on Trade and Development, Information Economy Report 2017 entitled 'Digitalization, Trade and Development' (UNCTAD, 2017). In this Report, it was perceived that with the increased reliance on digital technologies, such as cloud computing, three-dimensional printing, big data and "the Internet of things", most industries and global value chains would be transformed. Digital technologies not only create opportunities for new types of trade (in digitally traded products, services and tasks), it also boosts the sale of "traditional" trade as e-commerce and other online platforms boost the visibility of products and at times even match buyers and sellers. Services which enable the connection of buyers and sellers, such as those related to logistics, payments, market research, trade compliance, data for market intelligence, advertising, refunds and dispute resolution mushrooms by the day. (UNCTAD, 2015).

To survive in this digital economy, inevitably SMEs are required to adopt digital platforms in their services. The rise of Lazada as a premier online in Southeast Asia alludes the fact that to thrive in this digital economy, one has to tap on the nascent consumer market using an online business model. Lazada, headquartered in Singapore, was launched in 2012 as an online retailer and marketplace. By June 2017, it was operating in 6 South-East Asian countries: Indonesia, Malaysia, the Philippines, Singapore, Thailand and Viet Nam. Not to forget, of course, Alibaba, a Chinese company launched in 1999 that has transformed to be the biggest e-retailer in the world.

The Australian government, in a like manner, has also outlined certain strategic initiatives to tap on the positive force of the digital economy. In a report entitled, *The Digital Economy: Opening up the Conversation*, it was highlighted that among the things required for the regulators would be laws that enable and support the digital economy (Australian Law Reform Committee, 2018). In the Report, the term 'digital economy' is used to describe the range of economic and social activities that are enabled by information and communications technologies. From the government and business angle, areas of competitive strength must be built up in order to enhance digital readiness and capability and drive productivity. To support connectivity, interoperability and a single harmonized international standard on protocols and devices would need to be developed.

As a corollary, the rise of e-commerce and the prospect of full-blown digital economy challenges the traditional framework of commerce, as we know it. Any differences in domestic policy and legal framework would only exacerbate the problems further. This necessitates for the need to have

a uniform standard global rules that applies across the board. E-commerce, like global trade, must also be subjected to same global standards if e-commerce is to flourish. The ensuing issue would be what are the norms to be standardized, what institutions should champion norm setting and using which platform?

The paper is structured in this particular manner. Part two explores international initiatives to govern e-commerce particularly by the World Trade Organisation, the main body that regulates international trade at the global level. This is followed by an analysis of the Comprehensive and Progressive Trans-Pacific Partnership Agreement (CPTPP), particularly the Electronic Commerce chapter, a regional trade agreement that lays down substantial rules on e-commerce. The ensuing part investigates the implication of the CPTPP obligations on Malaysia before the conclusion ends the discussion.

2. ELECTRONIC COMMERCE AND TRADE AGREEMENTS.

The biggest global multilateral system, the World Trade Organisation (WTO), attempted to develop rules on e-commerce three decades ago, but until now has yet to come close to even framing any complete treaty. The prevailing perception is that the WTO rules governs only physical trade and has little to do with e-commerce. Regardless, some rules on privacy can be found in the founding agreement of WTO itself, i.e. the General Agreement on Trade in Services (1948). Article XIV(c)(ii) of the WTO's General Agreement on Trade in Services (GATS) permits trade restrictions that are necessary for "the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts", specifying that "such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services". Such provision necessarily means that although issues on privacy might already been in the radar of the WTO, but as e-commerce itself came through only in the mid-1990s, these rules were not drafted with e-commerce in mind.

Ever since the growth of Internet and E-commerce, several initiatives have been introduced by the WTO to govern trade involving digital goods. It started with the Information Technology Agreement in 1996. The Agreement, which is a plurilateral agreement was concluded in Singapore with 29 participants focusses on eliminating tariffs on IT products covered in the Agreement. The Agreement does not contain any substantive provisions on e-commerce and to breach this gap the WTO came up with "*Work Programme on E-commerce"* in 1998 (World Trade Organisation, 2018). The work programme entails an examination on all trade related issues arising from global e-commerce. Principally, it tried to come up with minimal standards on the legal eco-system surrounding e-commerce such as protection of privacy, prevention of privacy, protection and enforcement of copyright and trade mark and the complex rules of origin. More fundamentally, the work programme provides some clarity in terms of the important terminologies, the most important is the definition of e-commerce which has been defined as "*the production, distribution, marketing, sale or delivery of goods and services by electronic means".* The work at WTO on e-commerce is still ongoing with members submitting proposals at the Ministerial Conference.

In a number of disputes, the WTO panelists have sought to extend the traditional rules of law in GATT and GATS to cover digital products (Ryan T., Trachtman and Hudec, 2001). These cases include *United States-Measures Affecting the Cross Border Supply of Gambling and Betting Services* (*US Gambling*, 2004) on the applicability of the "public morals/public order" defense under the general exceptions of Article XIV of GATS, *Mexico-Measures Affecting Telecommunications Service (Mexico Telecommunications*, 2009) and *China-Measures Affecting Trading Rights and Distribution Services For Certain Publications And Audiovisual Entertainment Products (China-Audiovisual Products*, 2009). In *US Gambling*, Antigua and Barbuda raised a complaint regarding measures imposed by the US which affect cross border supply of gambling and betting services. In that case, even though online gambling does not typically fall within the traditional classification of trade in services nor trade in goods, the WTO Panel nevertheless found online gambling to be means of delivery included in mode 1 of GATS (i.e. cross-border supply) thus subjecting to WTO rules on trade. In *Mexico Telecoms*, certain measures relating to basic and value-added telecommunications services imposed by Mexico was alleged to have been anti-competitive and discriminatory. The decision of the Panel Body again attests to the fact that telecommunication measures fall within Mexico's GATS commitments and obligations specifically GATS Annex on Telecommunications. In *China-Audiovisual Products*, the subject matter of dispute were measures relating to a whole range of content, both in physical as well as digital. These measures were alleged to be inconsistent with GATS as they imposed burdensome and discriminatory rules on content review requirements necessary for the showing and viewing of content on national broadcasting services. In this case, the Panel applied the normal GATS rules to subject matter that includes digital content. As a whole, the 3 cases illustrate that the normal WTO trade rules, could a certain extent, be made applicable to digital materials. There is nothing in the WTO rules that deal specifically with substantive laws necessary for e-commerce to take effect and this is a major gap that the WTO itself is currently seeking to address in its Work Programme on E-Commerce as addressed earlier.

As WTO rules are developed along the traditional classification of trade in goods and trade in services, there is recurrent uncertainty as to whether electronic commerce is classified as goods or services. On that basis, Rolf H. Weber views that the legal framework of the WTO does not meet the regulatory need of the digital trade business (Weber, 2015). Another scholar, Burri argues that the WTO jurisprudence on e-commerce is patchy and fails to contribute to a sufficient level of legal certainty (Burri, 2017). Secondly, Burri felt that the WTO rules and system has failed to keep in touch with the latest development of digital technology. Burri, further lists down a series of issues which are yet to be made clear by the WTO including whether electronic commerce falls under GATS mode 1 (cross border) or mode 2 (consumption abroad)? Does the classification under WTO depends on the physicality of the goods traded, e.g. digital product recorded in a medium? Would it cover digital products delivered electronically? Weber, on the same note, agrees that the current WTO rules on global trade does not correspond with the dynamism of the digital revolution (Weber 2018).

Not surprisingly, countries started to champion the governance of e-commerce through free trade agreement (FTA), which started initially in the form of provisions on paperless trading (such as the Agreement between New Zealand and Singapore on a Closer Economic Partnership (2000); APEC Blueprint for Action on Electronic Commerce; Agreement between Japan and Singapore for a New Age Economic Partnership (2002)), then later as a full-blown e-commerce chapter (such

as Singapore- Australia Free Trade Agreement (SAFTA); Thailand with Australia and New Zealand (2004/2005); Japan-Philippines Economic Partnership Agreement (2006); Korea-Singapore Free Trade Agreement; Singapore- India Comprehensive Economic Cooperation Agreement (2006); Agreement between Japan and Australia for an Economic Partnership (2014); Agreement between Japan and Mongolia for an Economic Partnership (2015)). These FTAs which are primarily championed by the US since 2000 has a chapter on e-commerce. A study by WTO revealed that 75 FTAs representing 27% of all FTAs notified to the WTO contain provisions on e-commerce (Bieron & Ahmed, 2012). These provisions are deeply heterogeneous in nature, covering different aspects of e-commerce. Consequently, the US pushed for a specific e-commerce chapter that fortifies important rules on e-commerce in the form of Trans-pacific Partnership Agreement (TPPA). With the exit of US from TPPA, the remaining 11 members renegotiated the agreement by suspending certain provisions and the new agreement is called the Comprehensive and Progressive Trans-Pacific Partnership Agreement (CPTPP). The ensuing section discuss provisions of CPTPP on e-commerce.

3. THE ELECTRONIC COMMERCE CHAPTER OF CPTPP

The CPTPP which originated from the TPPA, was signed by 12 countries on 4 February 2016. Before TTPA's enforcement took effect, the US withdrew from the Agreement leading to the renegotiation of some of its controversial provisions. The renegotiations that started on the 21 May 2017 eventually found consensus on 9-10 November 2017 and targeted to be signed on the 8 March 2018. The official text of the Agreement was subsequently released for public viewing. The CPTPP maintains most of the original TPP Agreement, but some of the controversial provisions were suspended. Among the suspended provisions are those relating to government procurement (Article 15.8 (Conditions for Participation) and Article 15.24 (Further Negotiations), patentable subject matter (Article 18.37); patent term adjustment (Article 18.46 and Article 18.48) ; clinical data (Article 18.50); biologics (Article 18.51); extension of copyright term (Article 18.63); technological protection measures (Article 18.68); rights management information (Article 18.69) and protection of encrypted program-carrying satellite and cable signals (Article 18.79).

Not surprisingly, Chapter 14 that deals with electronic commerce was adopted in total. The TPP itself has been hailed as 'twenty first century' trade agreement and with respect to e-commerce, it has the most comprehensive advanced model for e-commerce. Burri, maintains that CPTPP covers a number of new issues not found in other international treaties, including: (i) domestic electronic transaction framework, (ii) the protection of personal information, (iii) internet interconnection charge sharing, (iv) location of computing facilities, (v) unsolicited commercial electronic messages, (vi) source code, and (viii) dispute settlement.

Structurally, the CPTPP can be divided into a number of fundamental components: (i)physical infrastructure (e.g. telecommunication system), (ii) domestic regulatory system (e.g. consumer protection, (iii) support services systems (e.g. payments, logistics and express delivery) and (iv) border regulations (e.g. duties, trade procedures) (Monteiro et al, 2017).

For the purpose of this paper, we will deal with the four components of the E-commerce chapter, i.e. (i) digital goods; (ii) domestic regulatory system (iii) computing facilities and (iv) cross border data transfer.

3.1. Digital Goods

Divergence in domestic regulatory system may inhibit the free flow of global e-commerce. The E-commerce chapter tries to harmonise national standards by containing a number of definitions and provisions that set to offer international norms on relevant provisions. Of most important is the meaning of 'digital products' that the Chapter sought to govern. As mentioned earlier, there is an uncertainty at WTO whether digital products should be classified as 'trade in goods' or trade in service. To arrest that uncertainty, the E-commerce Chapter defines 'digital products' to mean:

> *"'digital products' means products such as computer programs, texts, plans, designs, videos, images and sound recordings or any combinations thereof, that are digitally encoded and transmitted electronically."*

Another area of contention is whether national countries should be allowed to impose tax on e-commerce. The developing countries, in particular, would be able to garner a substantial income by imposing tax on e-commerce. The argument is that if import and export of goods is subjected to tariffs, then surely digital goods should equally be taxed. On this point, the E-Commerce Chapter paradoxically disallow any imposition of customs duties. This is consistent with the WTO standards that has imposed a permanent duty-free moratorium on electronic transmissions and their content as a result of the Nairobi Ministerial Conference in 2015 (WTO Doc.WT/MIN (15)/42(2015). As spelt out in Article 14.3, no custom duties shall be imposed on electronic transmissions which includes pure digital products that are transmitted electronically. Regardless, member countries are allowed to impose internal taxes, fees and other charges for digital content.

It is important that all effort to draw a distinction between trade in physical goods and trade in digital goods be eliminated. To achieve that, the Chapter establishes two fundamental concepts, non-discrimination which is contained in Article 14.4 and functional equivalence in Article 14.9. In terms of non-discrimination, the Electronic Commerce Chapter prescribes principles on access and use of the Internet for Electronic Commerce. This provision basically recognizes the right of consumers to have access to the Internet and freedom to access information on the Internet. With regards to technological neutrality, the Chapter prescribe member countries to not treat digital products less favourably in comparison to physical products. Member countries are mandated to accord similar treatment to digital products. Further in article 14.9, electronic trade administration documents must be considered to be the equivalent to paper versions.

3.2. Domestic Regulatory System

The second part of the chapter deals with domestic regulatory system. This part involves legal norms on e-commerce, electronic signatures, consumer protection, spam, personal information protection and paperless trading.

The first such provision relates to e-commerce law. It is imperative that national countries have some specific law on e-commerce and not just relying traditional rules on contract for it to take place effectively. On this ground, the E-Commerce Chapter mandates that parties should adopt

some national system on e-commerce law. There is no imposition of any standards or threshold, enough that they are consistent with the principles of the UNCITRAL Model Law on Electronic Commerce 1996 or the United Nations Convention on the Use of Electronic Communications in International Contracts. The imposition of UNCITRAL Model Law is not surprising as it contains a set of internationally acceptable rules and has been adopted by many national countries already. The Model law contains three fundamental principles that elevate e-commerce to be equal to trade in goods i.e. non-discrimination, technological neutrality and functional equivalence. In addition to that, the Model Law contains necessary components to establish the validity of an electronic transactions. These are rules pertaining to the formation and validity of contracts concluded by electronic means, for the attribution of data messages, for the acknowledgement of receipt and for determining the time and place of dispatch and receipt of data messages. Without these rules, the normal provisions on contractual formation could be resorted to and as a result may not fit easily with electronic contract.

The United Nations Convention on the Use of Electronic Communications in International Contracts which is entered into in 2005, builds on the provisions of UNCITRAL Model Law on E-Commerce. It reinforces the fundamental provisions laid down in the latter by adopting the same position with regards to non-discrimination, technological neutrality and functional equivalence. The basic purpose of the Convention, like the Model law is to eliminate any formal obstacle against electronic transactions.

The second area in need of harmonized rules is with respect to online consumer protection. The Electronic Commerce Chapter does not prescribe any specific threshold. It mandates that such laws must address 'fraudulent and deceptive commercial activities that cause harm of potential harm' to consumers. Such measures to combat online consumer fraud may include international cooperation, such 'mutual arrangement' or broader international frameworks to enhance consumer welfare.

The third area is with respect to personal information protection. Under the Chapter, the term *"personal information means any information, including data, about an identified or identifiable natural person".* The Agreement do not impose any threshold on the standards to be adopted, just that each party must have a proper legal framework for the protection of such data. The parties also must have a mechanism how individuals can pursue remedies and sufficient information must be published on how businesses can comply with any legal personal data/privacy requirements.

National countries have taken different approaches in protecting personal information. A number of international standards are available for personal data including the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980, the EU General Data Protection Regulation 2016 (GDPR) or the self-regulation system as practiced in the US. Some countries like Malaysia have adopted the more rigid EU approach in governing personal data, whilst others have in place certain data principles derived from the OECD guidelines. Consumers are extremely concerned over how their personal data are being collected, stored and used online and they genuinely fear for the loss of privacy online. It is important that coherent and uniform rules are being practiced worldwide for robust electronic commerce to take place. On this respect, the Chapter recognizes such divisive treatment on personal data by 'encouraging the development of mechanisms to promote compatibility between the different regimes. They may come in the form recognition of regulatory outcomes or broader international frameworks.

The fourth area relates to unsolicited commercial electronic messages or spam which can constitute an enormous amount of irritation to online users. Not only these spams clog the mail servers but they also cost money and time to be cleaned up. As many countries have yet to come up with any effective legislative provisions on spam, therefore the E-Commerce chapter mandates parties to introduce measures to allow users to not only prevent spam but to minimize spam. Under the chapter, the term "unsolicited commercial electronic message" is defined to mean "an electronic message which is sent for commercial or marketing purposes to an electronic address, without the consent of the recipient or despite the explicit rejection of the recipient, through an Internet access service supplier or, to the extent provided for under the laws and regulations of each Party, other telecommunications service". In this respect, there are two alternatives, the opt in approach and the opt out approach. The opt in approach requires consent to be obtained from the consumer as soon as data is collected whilst the opt out approach requires consent to be obtained at the point the personal data is to be shared to the third party thus enabling the consumer to opt out if he/she disagrees. The E-commerce Chapter takes these two options into account by giving options to member countries to adopt either one of the approaches. These measures should also address the issue of user's consent for the receipt of spam. Presently, there is no single standard mode in acquiring users' consent, even under the relevant national personal data protection legislation. The third option contained in the Chapter is the simple provision for the minimization of spam which could have been achieved using some technological tools.

3.3. Computing Facilities

Due to the cross-border nature of e-commerce, one of the requirements set by CPTPP is non-compulsion of usage or locate computing facilities in that Party's territory. To that extent, such requirement is different from data localization which refers to laws or policies that compel national companies to store and process data in data centers located physically within national border. The reason why national countries impose such a requirement is to arm them with the power to control their national's data to address not only national security concerns but to contain personal data within the jurisdiction. Data localization requirement is considered as trade protectionism measures and is heavily negotiated in free trade agreements. Selby, views that the imposition of data localization resulted rather from fear of losing out to more technologically advanced countries in terms of data hosting and internet signal intelligence, particularly the US (Selby, 2017). In the CPTPP, what is provided is with regards to the usage of computing facilities rather than data storage. Requirements on local data storage for the purpose of safeguarding the security and confidentiality of communications may be allowed under the general provision of Article 14.13 (1) of the CPTPP.

The restriction on the use of local computing is subjected to two broad qualifications. As provided under the CPTPP, any legal measures to require local computing facilities is allowed if it is necessary to achieve public policy objective on two requirements i.e.:

(a) It is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and
(b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective.

One major worry of ICT company in deciding whether to open up an offshore branch decision in a foreign territory is that the latter may impose domestic legislation to force the company to reveal or give up its valuable source code "for inspection" in order to have access to the other domestic market. The E-Commerce chapter forbids this practice in Article 14.17. This means government cannot insist on having access to the latter's source code even if there are security or inter-operability issues. Two exceptions have been struck for this obligation i.e. with regards to bespoke software and software used for critical infrastructure.

3.4. Cross Border Transfer of Data

The fourth component of the CPTPP deals with cross border transfer of information by electronic means. Data is the lifeblood of digital economy and without the free flow of data, global e-commerce would be a challenge. TPP is the first international treaty that establishes the link between privacy and trade. In this digital era, with the increasing needs of high volume of data, most Malaysian companies have moved to the cloud. With cloud computing technologies, where data is shared and transmitted across remote computers, transnational companies that operate beyond national borders would be transmitting and exchanging data across borders. This implicates that a company that uses a cloud computing service would be subjected to different national domestic privacy and data protection laws. There have been two examples where national countries have extra territorial powers to force cloud service providers to provide access to their data for national security or law enforcement purposes, i.e. United States Patriot Act and National Security Law of China. As national countries may have different threshold on the protection of personal data, cloud computing servers would be subjected to different national laws (Tian, 2016). In addition, most national legislation contains provisions on cross border data transfer, subjecting cloud providers to a patchwork of national laws on personal data protection.

To that extent, the CPTPP stands is that member countries should allow the cross-border transfer of information by electronic means. What is contentious however is that the obligation also extends to personal data. Over the past two decades, many national countries have come up with its own legislation to confer protection over personal data. With the proliferation of e-commerce, personal data is routinely recorded and transferred across national border, often for the simple purchase of consumer products. The divergence of national compliance requirements on personal data could increase the cost of doing business (UNCTAD, 2016). The European Data Protection Directive 1995(EU Directive 95-46-EC) provides for the most stringent obligation. The Directive requires express consent whenever personal data is sent and processed overseas. On the other hand, such strict rules may impede the free flow of data which is imperative in e-commerce. UNCTAD, for example, in its study on data protection laws around the world, emphasizes on the need to find an optimal balance between facilitating trade and security measures with regards to personal data (UNCTAD, 2016).

Burri asserts that the US's policy of prioritizing trade over privacy rights has resulted in the EU losing their case in *Schrens v Data Prot. Comm'r, Judgment of the Court*, (COM (2015) Case C-362/14, Schrens v Data Prot. Comm'r, Judgment of the Court, COM (2015), 566 final, Nov. 6. 2015, 21-23) before the Court of Justice of European Union (CJEU) that struck down the EU-Safe Harbor Agreement. One of the main reasons given for the judgement was that European data used

in digital business by US companies are not sufficiently protected in the United States (Wallace, 2016).

To that respect, the CPTPP seeks to reverse the finding of the CJEU by holding that national countries shall as a matter of policy 'allow any cross border of information by electronic means, including personal information, especially, when this activity is for the conduct of the business of a covered person'. This means free flow of data is seen to be more fundamental than any protective measures on cross border transfer of personal data as practiced in Europe and other national countries.

4. IMPLICATIONS OF THE CPTPP E-COMMERCE CHAPTER ON MALAYSIA.

The issues championed in the CPTPP Agreement are those that disrupt trade or increase the cost of doing business including data privacy, non-discrimination, technology neutrality, spam, cross border data flow and localization of computing facilities. This part investigates the implications of the CPTPP obligations on Malaysia. Malaysia has started regulating on cyberlaw beginning in 1997 with the establishment of the Multimedia Super Corridor. Among the earliest laws promulgated are the Computer Crimes Act 1997, Digital Signature Act 1997, Telemedicine Act 1997, Copyright Amendment Act 1997 and Communication and Multimedia Act 1998. Following a short gap, they are followed by the Electronic Commerce Act 2006, Electronic Government Activities Act 2007, Personal Data Protection Act 2010, the amendment to Evidence Act in 2012, the amendment to Consumer Protection Act 1999 in 2010, Special Offences (Securities Measures) Act 2012 and most recent is the Fake News Act 2018.

4.1. Digital Goods

In all these cyber-legislations, the term 'digital goods' is not given any specific treatment. The Electronic Commerce Act 2006 deals with electronic messages in commercial transactions, the Personal Data Protection Act 2010 deals with personal data in commercial transactions, the Communications and Multimedia Act 1998 deals with electronic communications and electronic content. The closest notion to digital goods may, however, be found in the wide rubric of 'goods' under the Consumer Protection Act 1999 as amended in 2010.

The notion of non-discrimination and net neutrality has been explicitly declared in s 3(3) of the Communications and Multimedia Act 1998 that there will be no censorship of the Internet. As for the functional equivalence between physical documents and electronic documents, this is provided for by the Electronic Commerce Act 2006.

On the moratorium on taxation on digital goods, the World Bank reports that Malaysia currently has limited means to tax cross-border transactions in the digital economy but has signed a multilateral convention in January 2018 to update on international tax rules. Certain activities are already subjected to taxation such as sourcing of content, procurement of goods, promotions, advertisement, selling, updating and maintaining the website, and uploading and downloading of content (World Bank, 2018). But these are all indirect taxes as imposing direct taxation could be problematic as the provider may be virtual and residing outside the country. As conceded by the

World Bank report, "the challenge is to modify the regime for indirect taxation so that it effectively captures the consumption of digital products services from foreign suppliers". Consequently, Malaysia is still exploring on how it could leverage on existing international tax rules to develop detailed solutions considering both direct and indirect taxation (World Bank, 2018).

4.2. Domestic Regulatory System

The CPTTP provides for four areas of domestic regulatory system. The first deals with the need to have a proper legal framework to govern electronic commerce. Two models were suggested by CPTPP i.e. the UNCITRAL Model Law on E-Commerce (UNCITRAL, 2018) and the United Nations Convention on the Use of Electronic Communications in International Contracts. In that respect, Malaysia decided to base her e-commerce law on UNICITRAL Model Law on E-Commerce. The Act which was promulgated in 2006, has extensive provisions on electronic contracts, including on formation and validity of contracts entered into by electronic means. It addresses all the formal requirements for such contracts to be considered as valid such as writing, signature, seal, witness, original, retention of documents, copy, prescribed form, service and delivery. It also addresses time of dispatch and place of receipt which is crucial in the formation of contract. Most important is the declaration that electronic information shall not be denied legal effect, validity, or enforceability just because it is in electronic form.

The second area deals with addressing consumer grouses and complaints for goods purchased online. On this respect, the Consumer Protection Act 1999 was amended in 2010. The Amendment extend all the rights conferred to consumer for goods purchased offline to the online environment. The Act confers consumers with the right to address misleading and deceptive conduct, false representation and fair practice, safety of goods and services and unfair contract terms. A number of guarantees or warranties are enjoyed by consumers with respect to purchased goods through online transactions similar to goods purchased in bricks and mortar, i.e. implied guarantee as to title, acceptable quality, fitness to a particular purpose, goods to comply with description, goods to comply with sample, implied guarantee as to price and repairs and spare parts.

The third area deals with protection of personal data. In this regard, Malaysia has her own data protection law, i.e. the Personal Data Protection Act 2010 ('PDPA 2010') which takes into effect on November 15, 2013. The Act has within its ambit a number of internationally recognized data principles i.e. Principles, General, Notice and Choice, Disclosure, Security, Retention, Data Integrity and Access Principles (Leo & Jeong, 20112; Azmi, 2007). As the Act drew provisions from the EU Directive, it prohibits the cross-border data transfer from Malaysia to other countries unless specified by the Minister (Section 129 of the PDPA 2010). At the moment, certain data transfer is allowed under the PDPA 2010, including:

- where the data subject has consented to the transfer;
- where the transfer is necessary for the performance of a contract between the data subject and the data user;
- where the transfer is necessary to protect the vital interests of the data subject; and
- where the data user has "taken all reasonable precautions and exercised all due diligence" to ensure that the personal data will not be processed in the recipient country in a way that would be a contravention of the PDPA (Section 129(3) of PDPA 2010).

> The definition of 'personal data' under the TCPPP is broader than the one under the Malaysian PDPA 2010. The CPTPP provision covers all '*information, including data, about an identified or identifiable natural person".* In that sense, expressions of opinion and any other information that could be attributed to an individual would be falling within the domain of personal data under the CPTPP. There are a number of areas whereby the PDPA 2010 is narrower than the TCPPP. Firstly, the Malaysian PDPA is restricted to information which is processed with respect of commercial transactions only. Secondly, the TCPP provisions do not specify the mode of processing of such data, whilst, the Malaysian PDPA focuses on data processed by electronic means. Thirdly, the Malaysian PDPA provision expressly excludes information relating to credit reporting business.

Another fundamental difference is that CPTPP does not have any special requirements on sensitive data. Under the said Act, sensitive data should not be processed unless explicit consent is obtained by the data subject. Other stringent rules apply to the processing of sensitive data as outlined under section 40 of the Act. The term 'sensitive data' under the Act refers to 'information as to the physical or mental health or condition of a data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence or any other personal data as the Minister may determine by order published in the Gazette'.

The fourth area provided by CPTPP is unsolicited bulk email or spam. Spam is a serious problem in Malaysia and it appears that Malaysians receive seven spam calls per month (Malaysian Digest, 2018). Section 43(1) of the Personal Data Protection Act 2010 arms the data subject with the right to request for the cessation or non-processing of his personal data for purposes of direct marketing. If the data user fails to comply with the request, the data user could be subjected to an offence which is punishable by fine and imprisonment (s43(4) of the PDPA 2010). One provision that often being used to combat unsolicited communications on the internet is section 233 of the Communication and Multimedia Act that deals with repeated communication with the intention to '*annoy, abuse, threaten or harass any person'*. As intent is prerequisite to this provision, it may be inadequate to deal with spam. The provision does not in any way confers civil sanctions for unlawful conduct.

4.3. Localization of Computing Facilities

The CPTPP contains a strong provision against the imposition of local computing facilities to businesses desiring to set up in member countries. The banning of localization of computing facilities under the CPTPP is not expected to give much problems to Malaysia as there is no such requirement under the existing law. Malaysian businesses are free to subscribe to any electronic services licensed under the Communications and Multimedia Act 1998 and are thus free to take up offshore cloud service. However, the existing restraint on the cross-border flow of personal data under the Personal Data Protection Act 2010 might be perceived as a legal requirement that personal data is to be stored only in Malaysia and could only be transferred overseas on the fulfillment of certain requirements only.

4.4. Cross Border Data Flow

With regards to cross border data flow, the PDPA 2010, section 129 expressly disallow the 'transfer of personal data to a place outside Malaysia, unless to such place as specified by the Minister'. In principle, this would include a place that has in force any law that is substantially similar to PDPA 2010 'or that serves the same purposes' or 'ensures an adequate level of protection'. A strict interpretation of this provision requires a determination of the state of protection of personal data in the country of export. In that respect, the Commissioner is currently planning to formulate a White List, consisting of countries where such transfer is allowed (Public Consultation Paper No. 1/2017 & Lovells, 2018) In the Consultation paper published by the Commissioner, among the factors considered in the White List are:

(i) countries with comprehensive data protection laws in place
(ii) countries subjected to binding commitments in international treaties
(iii) countries with code of practice of national co-regulatory mechanisms in place.

In other respect, it is possible for personal data to be transferred to outside jurisdiction if consent has been obtained from the data subject as underlined under section 129(3). The transfer is also allowed if it is necessary for the performance or conclusion of a contract between the data subject or data user of a third party. Data transfer may also be necessary for the purpose of legal proceedings or obtaining legal advice and in such instance allowed under section 129(3)(d). Subsection (e) and (f) provides further areas where transfer of personal data is allowed. With that broad allowance, the PDPA 2010 prohibitions on cross border data transfer is not so stringent after all.

5. CONCLUSION

The World Bank in its 2018 report describes Malaysia's rapid accession from manufacturers and exporter of electronics and electrical equipment to the adoption of digital technologies as a remarkable success (World Bank 2018). The establishment of e-business has tripled between 2010-2015 (World Bank 2018). Unfortunately, the rate of adoption of the internet among the business is not as promising as the government. The Report cites how relatively few business establishments engage with the Internet. For businesses that participates in e-commerce, they are led by the manufacturing sector.

The free flow of data is key to regional digital trade, especially in the new 21st century global trade environment. The E-Commerce chapter tries to harmonise standards on digital goods, domestic regulations, location of computing facilities and cross border data flow. To that extent, the CPTPP which contains relevant substantive provisions on e-commerce constitutes an important trade initiative to iron out discrepancies between contracting parties that may disrupt trade or increase the cost of doing business. As examined earlier, hard obligations in the form of treatment of digital goods, the non-differentiation between physical goods and digital goods and net neutrality are three fundamental principles for e-commerce to prosper. The CPTPP also lays down substantive provisions that governs domestic regulation including on e-commerce, online consumer disputes, personal data protection and spam. In all these areas, Malaysia with its suite of e-commerce related legislation seems poised to have fulfilled all the expectations of CPTPP. The same thing could be said with the requirement of non-imposition of local computing facilities and cross border transfer of data. What may be required, perhaps, is just to accelerate on the White List

as this would provide clearer guidance on the countries to where such transfer is allowed, and this may perhaps, include all the CPTPP countries so as to comply with the E-Commerce chapter.

ACKNOWLEDGEMENTS

The project has been funded by Ministry of Higher Education (Malaysia) under the FRGS project (FRGS/1/2015/SSI10/UIAM/01/1)

REFERENCES

Azmi, I. M. A. G (2007). E-commerce and privacy issues: An analysis of the personal data protection bill. *International Review of Law Computers and Technology*, *16*(3), 317-330.

Australian Law Reform Committee (2018). *Digital economy*. Retrieved from https://www.alrc.gov.au/publications/3-policy-context-inquiry/concept-digital-economy

Bieron, B., & Ahmed, U. (2012). Regulating e-commerce through international policy: Understanding the international trade law issues of e-commerce. *Journal of World Trade, 46*(3), 545-570.

Burri, M. (2017). The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation. 51, *U.C.D.L. Rev* 65.

China-Measures Affecting Trading Rights and Distribution Services For Certain Publications And Audiovisual Entertainment Products (WTO Appellate Body Report, 2009).
https://logisticsofthings.dhl/sites/default/files/malaysiaecomm_infographic2017_0.png

Lovells, H. (2018). Malaysia publishes draft "white list" for personal data exports. *Lexology.* Retrieved from https://www.lexology.com/library/detail.aspx?g=dd479a7c-c346-43b4-9f98-ea424333f12b

Malaysian Digest. (2018). *Malaysians currently suffered the most spam phone calls in the region.* Retrieved from http://malaysiandigest.com/features/704975-malaysians-currently-suffer-from-the-most-spam-phone-calls-in-the-region.html

Maximillian Schrems v Data Protection Commissioner (CJEU, 6 October 2015) Retrieved from https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf

Mexico-Measures Affecting Telecommunications Services (WTO Panel Report, 2004).

Ministry of International Trade and Industry. (2018). *Trans-Pacific Partnership Agreemen*t. Retrieved from http://fta.miti.gov.my/miti-fta/resources/Text%20of%20TPPA%20(160516)/14._Electronic_Commerce_.pdf

Monteiro, Jose-Antonio., & Teh, R. (2017). Provision on electric commerce in regional trade agreement. *Econstor.* Retrieved from https://www.econstor.eu/bitstream/10419/163426/1/894047426.pdf

Oxford Dictionary. (2018). *British and world English.* Retrieved from https://en.oxforddictionaries.com/definition/digital_economy

Selby, J. (2017). Data localization laws: Trade barriers of legitimate responses to cyber-security risks, or both? *International Journal of Information Technology*, *25*(3), 213-232.

Tian, G. Y (2016). Current Issues of Cross Border Personal Data Protection in the Context of Cloud Computing and Trans-Pacific Partnership Agreement: Join or Withdraw. 34 *Wis. Intl'L.J.* 367.

United Nations Conference on Trade and Development. (2015). *Information economy report 2015: unlocking the potential of e-commerce for developing countries*. New York and Geneva: United Nations.

United Nations Conference on Trade and Development. (2016). *Data protection regulations and international data flows: Implications for trade and development*. New York and Geneva: United Nations

United Nations Conference on Trade and Development. (2017). *Information economy report 2017: Digitalisation, trade and development.* New York and Geneva: United Nations.

United Nations. (2018). *United Nations Convention on the use of electronic communications in international contracts.* Retrieved from https://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf

United States-Measures Affecting the Cross Border Supply of Gambling and Betting Services. (WTO Dispute Settlement Body, 2004).

Wallace, S. L. (2016). Rethinking Data Security: The Differences Between the European Union and The United States' Approach to Data Security and Building Transnational Standards with Transparency and Uniformity. 34 *Wis. Inty'l L. J*. 446.

Weber, R. (2015). Digital Trade and E-Commerce: Challenges and Opportunities of the Asia Pacific Regionalism, 10 *Asian J. WTO & Int'l Health L & Pol'y*, 321

Weber, R. (2018). The expansion of e-commerce in Asia Pacific trade agreements. *International Centre for Trade and Sustainable Development.* Retrieved from https://www.ictsd.org/opinion/the-expansion-of-e-commerce-in-asia-pacific-trade-agreements

World Bank Group. (2018). *Malaysia's digital economy: A new driver of Development*. Washington, DC: World Bank.

World Trade Organisation. (2018). *Work programme on electronic commerce 1998*. Retrieved from https://www.wto.org/english/tratop_e/ecom_e/wkprog_e.htm