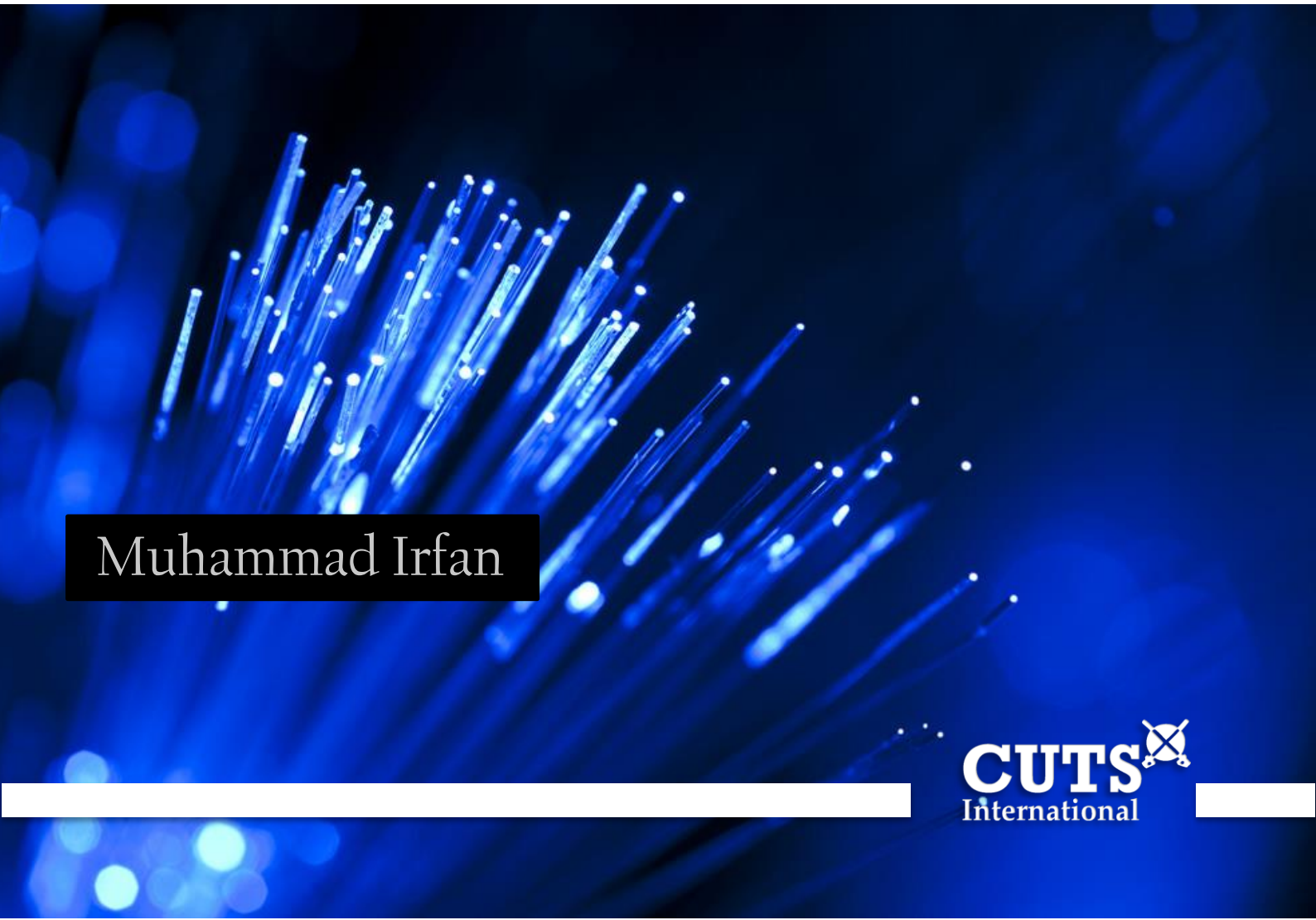
STUDY

Data Flows, Data Localisation, Source Code

Issues, Regulations and Trade Agreements



Muhammad Irfan

CUTS International

Data Flows, Data Localisation, Source Code: Issues, Regulations and Trade Agreements

Authored by:

Muhammad Irfan

Published by:

CUTS INTERNATIONAL, GENEVA
Rue de Vermont 37-39
1202 Geneva, Switzerland
www.cuts-geneva.org

This paper was undertaken by Muhammad Irfan, Counsellor, Permanent Mission of Pakistan to the World Trade Organisation. It is published under CUTS Internataional Geneva's project "Geneva Trade & Business Connexion: Mainstreaming Micro, Small & Medium Enterprises (MSMEs) into the Multilateral Trading System", undertaken with funding support from Australian Aid.

Citation: IRFAN, M. (2019). *Data Flows, Data Localisation, Source Code: Issues, Regulations and Trade Agreements*. Geneva: CUTS International, Geneva.

Table of Contents

Acronyms

CPTPP	Comprehensive and Progressive Agreement for Trans-Pacific Partnership
DRP	Data Regulation Policy
EC	European Commission
EU	European Union
FOSS	Free and Open Source Software
FTA	Free Trade Agreement
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit
MC	Ministerial Conference
OSS	Open Source Software
RTA	Regional Trade Agreement
UNCTAD	United Nations Conference on Trade and Development
USITO	United States Information Technology Office
USMCA	United States, Mexico and Canada Agreement
USTR	United States Trade Representative
WTO	World Trade Organisation

Executive Summary

Advancements in digital technology have revolutionised economic activity in the 21st century. E-Commerce has emerged as an important medium of domestic and international trade. While these developments present several opportunities, harnessing the technologies for economic development pose new legal and regulatory challenges for countries in their trade and industrial policies.

Current patterns of digital trade are heavily skewed in favour of advanced countries. This is due to their superior digital infrastructure and capabilities compared to the rest of the world, pointing to a 'digital divide'. Effective domestic policies may be required to address this in order to reap the dividends of the latest digital developments.

The subject of E-Commerce has received attention during various international discussions, including those at the WTO. Issues related to regulatory policies on data and technology have proved particularly complex and controversial. Such debates address the regulation of data flows, data localisation, sharing of source-codes and similar policies on digital technology.

The emerging importance of data in modern times resembles that of oil in the 20th century, symbolising its power as an economic resource, and its ability to define political economy relationships. Control over data, thus, presents a key issue. Some countries use data localisation policies and other regulations on data flows to develop their own digital industry. Those with already developed industries see such regulations as restrictions on trade and constraints to the full realisation of free trade.

Similarly, the issue of sharing source code has attracted much attention. Source code, algorithms, and encryption techniques embody the technology driving digital innovation. They are seen as vital for the development of modern industries. Some countries demand disclosure of source code along with other technology and performance requirements in their national policies. Countries already possessing such technological prowess see these policies as restrictive for trade and investment.

Attempts have been made to bring these issues into trade agreements. At the WTO, some countries have recently been discussing them with a view to framing new rules. A few countries have already incorporated such provisions in Regional Trade Agreements (RTAs). These provisions seek to restrict – in varying degrees and exceptions - countries from using policies on data localisation or source code disclosure.

The issues are complex and there is no one-size-fits-all solution. Similar debates on conventional trade have taken place before and still continue, albeit with mixed results. The real test for developing countries would be how they balance the necessity of domestic policies for digital industrialisation against the demand for international trade discussions and negotiations.

SECTION 1

Background

Trade and industry have long remained key drivers of the global economy. Simultaneously, improvements in technology have continually given rise to new industries and altered the ways in which trading takes place. Recent technological advancements have ushered in a new digital era which has revolutionised economic activity around the world. Digital technology has dramatically increased the speed of production and communication, enabled new production processes, altered international value chains and posed new challenges for countries in their trade and industrial policies.

These developments present great opportunities for governments to rapidly develop their economies by expanding businesses, integrating into value chains, and connecting remote areas both across the globe and within their countries. In order to do that, however, countries increasingly require a robust digital infrastructure, different skill-sets, newer technological capabilities and production capacities to exploit these technologies. This presents various policy challenges in the form of legal and regulatory frameworks both at the domestic and international level.

This paper explores a few of the complex regulatory concepts that have emerged within the domain of E-Commerce in recent times to enhance their understanding and highlights different ways in which some countries have dealt with the issues in their national policies and trade agreements. It also aims to provide a brief summary of the pros and cons of the available policy options.

E-Commerce is a noticeable feature of the rapidly developing digital economy. There are varying ways in which it is defined, but it is generally understood to encompass activities related to the buying and selling of goods electronically. The WTO defines it as the "production, distribution, marketing, sale or delivery of goods and services by electronic means."[1]

While it has proved hard to measure in its entirety, UNCTAD (2017) has estimated[2] that global e-commerce sales in 2015 were close to $25.3 trillion. Almost 90% of these (around $22.4 trillion) were accounted for by B2B (Business-to-Business) E-Commerce. The share of B2C (Business-to-Consumer) sales was $2.9 trillion.

The country-wise distribution shows very high concentration in the more economically advanced economies. Of the $25.3 trillion, the top ten economies[3] account for 64%. This is attributable to the large gap between digital infrastructure and capabilities of these countries compared to the rest of the world. Indeed, various analyses point to the existence of a stark digital divide between developed and developing countries heavily skewing the current state of E-Commerce in the favour of the former.

The subject of E-Commerce has been under discussion in the WTO since 1998 when the Work Programme on E-Commerce was formally launched in order to "examine all trade-related

[1] WTO Work Programme on E-Commerce' (WTO 1998) WT/L/274, para. 1.3.

[2] UNCTAD Information Economy Report, 2017.

[3] United States, Japan, China, South Korea, Germany, United Kingdom, France, Canada, Spain and Australia.

issues relating to global electronic commerce"[4]. The subject gained momentum before the Ministerial Conference in 2017, when some countries called for the launch of negotiations for multilateral rules on E-Commerce. The issue of negotiations remained contentious as several countries opposed the idea of fresh rules. However, during MC-11, a group of countries signed a Joint Statement to conduct exploratory discussions with a view to launching future negotiations on E-Commerce rules[5]. Countries carried out discussions under this Joint Statement initiative during 2018 over several meetings. At the end of 2018, there were calls for elevating these discussions to the level of negotiations among parties that intended to do so. Resultantly, on the side-lines of a WTO Mini-Ministerial organised in Davos, a group of countries signed another Joint Statement confirming their "intention to commence WTO negotiations on trade-related aspects of electronic commerce"[6]. It is still unclear what the result of the negotiations would be and what legal form any resulting agreement or negotiated outcome might take.

During various international discussions on the subject of E-Commerce, including those in the WTO, several issues have come to the fore concerning the conduct of cross-border digital trade. Among those, certain issues related to regulatory practices and policies on the aspects of data and technological aspects have proved complex and controversial at the same time. In particular, a debate has emerged on data flows, data localisation, source-codes and regulations on digital technology. The remainder of this paper will explore these issues with a view to understanding the issue, highlighting prevalent practices and discussing possible pros and cons of the arguments surrounding them.

[4] Declaration on Global Electronic Commerce (25 May 1998) WT/MIN(98)/DEC/2.

[5] Joint Statement on E-Commerce (13 December 2017) WT/MIN(17)/60 signed by 70 countries (EU = 28).

[6] Joint Statement on Electronic Commerce, (25 January 2019) WT/L/1056 signed by 76 countries (EU = 28).

SECTION 2

Regulatory Issues concerning Data

2.1 Data

The key building blocks of a digital economy are digital infrastructure and digital capabilities. Three interrelated components of digital infrastructure have been identified as networks, software and data.

While a concrete definition or meaning of the term lacks clarity, data is generally referred to as information in digital form and is understood to form the basic unit of the digital economy that allows it to function. It is data which provides platforms with the raw material they need to operate. With the evolution of the digital economy, the importance of data in modern times has become well-established. It is often referred to as the 'oil' of the twenty-first century[7] denoting its power as an economic resource, and its ability to define political economy relationships in international economic affairs. Others call it the fuel of the digital age, since its control unravels vast profit-making opportunities for its owners[8]. Some refer to it as the 'currency' of the digital economy highlighting its intrinsic economic value[9].

Data may be classified as personal and non-personal. Personal data refers to information on consumers, their education, health and consumer choices. Non-personal data may vary and contains more general information on certain sector or industry. The distinction is important from a policy point of view, as different regulations may be required for different types of data.

Rapid developments with respect to the speedy transfer of large volumes of data, its storage, analysis, and ultimate utilisation has created new regulatory issues and challenges including protection of privacy, large-scale commercialization by tech companies, cyber-security threats, unequal development of digital infrastructure and capacity, and several other concerns.

One of the most controversial features of the recent debates surrounding data relate to data flows and storage. This is natural, given the intrinsic potential of data to generate profits for businesses and contribute to national economies. Therefore, ownership, or control over data has become a key issue.

2.2 Data Flow and Storage

Just as data is defined as information in digital form, the flow of data can be termed as the movement of information in digital form. Data may flow from one computing facility to another enabled through the ICT infrastructure. This movement could be within or across national borders. During its journey, the data is required to be physically stored in servers or data centres. The speed and efficiency at which the data flows from the first point to the last depends on the superiority of the ICT infrastructure and

[7] Parkins, D. "The World's Most Valuable Resource", The Economist, 6 May 2017.

[8] Tarnoff B. "Big data for the people: It's time to take it back from our tech overlords", The Guardian, 14th March 2018.

[9] Eggers, W.D., Hamill, R. and A. Ali, "Data as the New Currency - Government's Role in Facilitating the Exchange", Deloitte Review, Issue 13, 2013.

technology. This means that often, companies that use data more heavily are located in countries that have better digital infrastructure[10].

As a natural consequence, countries that have better digital infrastructure are often in a better position to trade in data-intensive sectors and utilise the data more effectively[11]. Often, such countries would argue in favour of allowing free flows of data and removing any restrictions or barriers to the movement or storage of data.

However, there are several reasons for countries to regulate the flow of data, by placing barriers, restrictions or conditions on the movement at any stage. These could be for the protection of privacy of citizens through protection of their data, for national security reasons to protect sensitive or strategic information, and for achieving employment, industrial or technological development objectives by using localisation requirements.

Data Localisation, therefore, has emerged as a topic of intense debate. It refers to any legal limitations on the ability of data to move globally and/or to remain locally within the geographical boundaries of a country[12]. Data localization can be explicitly mandated in a country's law or it could be brought into effect through other policies or conditions, such as requiring companies to store a local copy of the data before transferring, making companies process data locally through local or locally partnered companies, and making it compulsory to gain individual and/or government consent for data transfers.

For the purpose of industrial development objectives, localisation works in the same way as local content requirements in conventional trade and investment policies. The aim is to make foreign companies with advanced capabilities and infrastructure invest with local partnerships, and for local companies to understand and utilise the superior technologies to develop local capabilities. This contributes to local employment and skill development.

Another argument for regulating the flow of data is to gain data-ownership. If the ownership of data rests with a few private sector-players, the risk of exacerbating information inequality becomes high as the same few companies would have the capacity to harness and handle the data while others would lose out[13]. Ownership of data at the national level can allow governments control over where and whom the data is used by and who it can be shared with. This can allow the data to be used specifically in some manufacturing processes, the development of local digital platforms, building data infrastructures, data processing skills and to be used in provision of public goods more efficiently.

While UNCTAD (2018)[14] has advocated the importance of protecting personal data, it also argues for non-personal data to be allowed to move freely within the country and to be shared at the regional level to encourage south-south cooperation. This can allow pooling of resources and overcome the entry barriers imposed by giant global tech companies.

In other quarters, regulation of data has found support only to the extent of following legitimate

[10] Sen, N. "Understanding the Role of the WTO in International Data Flows: Taking the Liberalization or the Regulatory Autonomy Path?" Journal of International Economic Law, Vol 21, Issue 2, 1 June 2018, 323–348.

[11] van der Marel, E. "Disentangling the Flows of Data: Inside or Outside the Multinational Company", European Centre for International Political Economy (ECIPE), Occasional Paper, 7/2015.

[12] Meltzer, J. "A New Digital Trade Agenda", E15 Initiative 2, 2015.

[13] GIZ (Deutsche Gesellschaft für Internationale Zusammenarbeit), "Data for development: What's next? Concepts, trends and recommendations for German development cooperation", November 2017.

[14] UNCTAD, Trade and Development Report, 2018.

public policy objectives, such as privacy, security and personal data protection. Even these objectives should not be used a disguised restriction on digital trade. Many countries have often used this narrative during trade negotiations.

Meanwhile, those who call for unrestricted data flows point to the ability of data to generate large profits and incomes, which should not be restricted. Cory [15] argues that such policies amount to "data protectionism" by creating new barriers to digital trade. This makes data flow more expensive and puts foreign firms at a disadvantage, keeps foreign competitors out of domestic markets and hinders particularly the ability of small firms to trade.

In terms of investment and technology, countries using such data localisation policies are likely to impose high costs on their own development by keeping investors at bay and making technology more expensive to use. This in turn, has a negative impact on GDP growth[16].

2.3 National Policies to Regulate Data Flows and Localisation[17]

Regardless of the arguments in favour or against the regulation of data flows, several countries across the globe, have enacted various laws to restrict the flow of data in one form or another and due to one or more of the above reasons. A brief summary of some of these policies is given below:

Rwanda

Rwanda has recently developed a Data Revolution Policy (DRP)[18] to be executed over five years from 2017 to 2022. The stated vision of the Rwandan government is to build an innovation-data-enabled industry to harness rapid social economic development. The policy contains a series of legal, policy and regulatory instruments addressing different aspects of digital trade. A Ministerial Order No. 001/MINICT/2012 of 12 March 2012, provides that all critical information data within Government should be hosted in one central national data centre. The organic law on statistics No. 45 of June 2013 stipulates mechanisms for coordination of statistical articles with regard to production, access and dissemination of data. The Penal Code and Law No. 18/2010 of 12 May 2010 relating to Electronic Messages, Electronic Signatures and Electronic Transactions deals with personal data protection, privacy and confidentiality matters.

Together, the instruments are designed for Rwanda to retain exclusive sovereign rights on its national data with control and power over its own data. The policy, however, allows, only under agreed terms and governed by Rwandan laws, to host its sovereign data in a cloud or a co-located environment in data centres within or outside of Rwanda.

The DRP also recognizes the importance of building a strong collaborative framework between Government and private sector at local, regional and international levels for fostering data-enabled technology innovations; establishing a data portal warehouse; establishing a framework

[15] Cory, N. "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" Information Technology and Innovation Foundation (ITIF), May 1, 2017.

[16] OECD "The Economic Impact of Local Content Requirements "Trade Policy Note, February 2016. https://www.oecd.org/tad/policynotes/economic-impact-local-content-requirements.pdf.

[17] Unless otherwise indicated, the following policy measures of each country have been compiled from various sources: Cory (2017), Sen (2018), USTR (2017).

[18] National Institute of Statistics of Rwanda (http://statistics.gov.rw/publication/rwanda-national-data-revolution-and-big-data)

to develop human capital in data science; and conducting big data analytics and business intelligence.

Turkey[19]

Turkey has, in the last few years made legislation to regulate both personal data and data in the financial and taxation sectors. In 2013, Turkey enacted the Law on Payments and Security Settlement Systems, Payment Services and Electronic Money Institution. It mandates Internet-based payment services, such as PayPal, to store all data in Turkey for ten years.

In 2016, Turkey enacted the Law on the Protection of Personal Data, which limits transfer of personal data out of Turkey and may require firms to store data on Turkish citizens in country. The law makes it compulsory for data controllers and processors to obtain "express consent" from individuals to transfer personal data to another country. The need for specific and individual engagement holds the potential to act as de facto data localization. Turkey's new law adopts a country-by-country assessments of privacy protections. The "Data Protection Board" will assess whether other countries provide an "adequate" level of privacy protection. Under this law, if the country receiving data from Turkey does not offer "adequate" protection, the Data Protection Board must provide permission for each transfer.

China[20]

China's data related laws have been evolving over time and new laws are being drafted regularly to improve on earlier ones. China employs a wide range of data regulation policies which cover financial, cloud-computing, privacy, and security related provisions. Most of these laws require companies to keep their servers in China, prohibit the off-shore analysis and or processing of Chinese personal financial information, and protect the medical, health and insurance related information of citizens.

Other than that, the Ministry of Public Security runs the Golden Shield program (commonly referred to as the "Great Firewall of China"), to restrict data imports by disallowing access to certain websites and services.

In 2016, it extended the localisation requirement servers used for online publishing including app stores, audio and video distribution platforms, online literature databases, and online gaming.

Also, China's new Counter-Terrorism Law requires Internet and telecommunication companies and other providers of "critical information infrastructure" to store data on Chinese servers and to provide encryption keys to government authorities.

Indonesia[21]

Indonesia also has a wide range of data-localization laws covering various sectors and technologies. In 2012, Indonesia enacted a regulation regarding the Provision of Electronic System and Transactions, which requires "electronic systems operators for public service" to store data locally. In 2014, Indonesia's central bank enacted a rule that requires e-money operators to store data locally.

Indonesia's Ministry of Communications and Informatics issued Circular Letter No. 3 of 2016, notifies over-the-top service companies (such as

[19] Ibid 17

[20] Ibid 17, Sacks (2018).

[21] Ibid 17; Kelsey, J., "The Risks for ASEAN of New Mega-Agreements that Promote the Wrong Model of E-Commerce, ERIA Discussion Paper Series, 2017 https://think-asia.org/bitstream/handle/11540/7662/ERIA-DP-2017-10.pdf?sequence=1

Skype and WhatsApp) about new regulations, including the requirement to store data locally.

Indonesia's Technology and Information Ministry has also issued regulation 20/2016 on personal data protection that stated that electronic system providers are required to process protected private data only in data centres and disaster recovery centres located in Indonesia.

United States

US data localization requirements mostly focus on public procurement. In 2016, the U.S. Internal Revenue Service issued publication 1075—Tax Information Security Guidelines for Federal, State and Local Agencies—which demanded that federal agencies must restrict the location of information systems that receive, process, store, or transmit federal tax information to areas within the United States territories, embassies, or military installations." [22] In 2015, the U.S. Department of Defense issued rules that require cloud-computing service providers working for the department to store data domestically[23].

Similarly, some state and local governments impose certain requirements. The City of Los Angeles, for example, required Google to store its data within the continental United States as a condition of its contract with the city.[24]

South Korea[25]

A Personal Information Protection Act requires companies to obtain consent from "data subjects" (i.e., the individuals associated with particular data sets) prior to exporting that data. The act also requires "data subjects" to be informed of who receives their data, the recipient's purpose for having that information, the period that information will be retained, and the specific personal information to be provided.

Korea has used data localization requirements to protect local e-commerce and online payment operators. In 2014, South Korea enacted an Act on the Establishment, Management, Etc. of Spatial Data. This prohibits mapping data from being stored outside the country due to security concerns[26]. Also, in 2015, Korea enacted the Act on Promotion of Cloud Computing and Protection of Users. Subsequent guidelines contain rules that effectively require data localization as cloud computing networks serving public agencies have to be physically separate from networks serving the general public.

Vietnam[27]

Vietnam has employed several, extensive data-localization policies as part of broad efforts to control Internet-based activities. Vietnam forbids direct access to the Internet through foreign ISPs and requires domestic ISPs to store information transmitted on the Internet for at least 15 days.

A new legalisation covers over-the-top services (such as WhatsApp and Skype) in a forced data-localization requirement. Decree 72 of 2013, requires a broad range of online companies (such as social networks, online game providers, and

---

[22] Internal Revenue Service, "Publication 1075: Tax Information Security Guidelines for Federal, State and Local Agencies", Washington, DC: September, 2016, https://www.irs.gov/pub/irs-pdf/p1075.pdf.

[23] Department of Defense, "Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018)", Washington, DC, August 26, 2015, https://www.federalregister.gov/documents/2015/08/26/2015-20870/defense-federal-acquisitionregulation-supplement-network-penetration-reporting-and-contracting-for

[24] Office of the City Clerk, City of Los Angeles "City of Los Angeles: Supplemental Report – Information Technology Agency Request to Enter into a Contract with Computer Science Corporation for the Replacement of the City's Email System," http://clkrep.lacity.org/onlinedocs/2009/09-1714_rpt_cao_10-7-09.pdf.

[25] Ibid 17.

[26] Ministry of Land, Infrastructure and Transport, "Act on the Establishment, Management, etc. of Spatial Data", 2014, http://elaw.klri.re.kr/eng_service/lawView.do?hseq=32771&lang=ENG.

[27] Ibid 21, OECD 2017

general information websites) to have at least one server in Vietnam.

India[28]

India has also enacted a range of laws and regulations requiring data localization. India's Ministry of Communications and Technology enacted data transfer requirements as part of a 2011 change to privacy rules that limit the transfer of "sensitive personal data or information" abroad to only two restrictive cases—when "necessary" or when the subject consents to the transfer abroad.

In 2012, India enacted a "National Data Sharing and Accessibility Policy," which effectively means that government data must be stored in local data centres. The Companies (Accounts) Rules law of 2014 also requires backups of financial information, if primarily stored overseas, to be stored in India.

A National Telecom Machine-to-Machine roadmap was released in 2015 that requires all relevant gateways and application servers that serve customers in India to be located in India. The roadmap has not yet been implemented. Indian government agencies have also made data localization a requirement for cloud providers computing for public contracts, through guidelines issues by India's Department of Electronics and Information Technology in 2015.

2.4 Provisions in Trade Agreements Covering Data Flows and Localisation

While many countries have instituted a diverse range of national policies to regulate the flows, storage or ownership of digital data, the issue has also surfaced in some Regional Trade Agreements. By the end of 2018, a total of 291 RTAs had been notified to the WTO and were in force. Around 25 per cent of them contain a specific chapter on electronic commerce. Provisions relating to customs duties, definitions and cooperation are among the most common categories found in the e-commerce chapters of these RTAs. Some RTAs also contain provisions on consumer/personal data protection, and non-discriminatory treatment for digital products. Issues related to source code and localization feature only in a few agreements.

As opposed to the national policies which seek to regulate data flow and localise its storage, RTAs covering data issues are mainly designed to restrict countries from using such policies. Ironically, many countries that have employed regulatory policies on digital data are also signatories to such RTAs. A brief summary of some RTAs is given below:

Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)

The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), is a trade agreement between 11 countries namely, Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, and Vietnam. 7 of the 11 countries have ratified the agreement.

On 'Cross-Border Transfer of Information by Electronic Means'[29], the parties recognise that

[28] Ibid 17

[29] Article 14.11 CPTPP available at https://www.mfat.govt.nz/assets/Trans-Pacific-Partnership/Text/14.-Electronic-Commerce-Chapter.pdf

each Party is entitled to its own regulatory requirements concerning the transfer of information by electronic means. However, each party must allow such cross-border transfer of information (including personal information), when this activity is for the conduct of the business.

Parties are not prevented from violating the above requirements to achieve a legitimate public policy objective, provided that their measures do not constitute arbitrary or unjustifiable discrimination or a disguised restriction on trade and do not impose restrictions on transfers of information greater than those required to achieve the public policy objective.

On 'Location of Computing Facilities'[30], parties recognise that each Party may have regulatory requirements to ensure the security and confidentiality of communications. However, no party can require to use or locate computing facilities in its territory as a condition for conducting business in that territory. The same caveat regarding legitimate public policy objectives applies in this case as well.

Korea-US FTA

This FTA only covers cross-border information flows. While recognizing the importance of the free flow of information in facilitating trade, and acknowledging the importance of protecting personal information, both parties agreed to endeavour to refrain from imposing unnecessary barriers to electronic information flows across borders[31].

Pacific Alliance FTA

This FTA has been concluded among Latin American countries along the Pacific Rim, i.e. Chile, Colombia, Mexico and Peru.

On Cross-border transfer of information, it contains almost similar provisions to that of the CPTPP. The only difference is that the test of *'greater than those required to achieve the legitimate public policy objective'* in the CPTPP is not mentioned in this FTA[32].

As with the CPTPP, this FTA also has the same provisions for data localisation. However, a footnote in the agreement clarifies that in case of investment, parties may make location related conditions[33].

Peru-Australia FTA

This FTA also contains effectively the same language as that of CPTPP and the Pacific Alliance on both cross-border transfer of information by electronic means and the location of computing facilities. [34] However, a caveat makes the provisions subject to chapter-wide and obligation-specific carve outs contained in the Scope and General Provisions, such as non-conforming measures on investment and trade in financial services[35]. Moreover, the provisions are also subject to any general exceptions in the agreement, for example, security and public policy[36].

---

[30] Article 14.13 CPTPP

[31] Article 15.8 of Korea-US FTA https://ustr.gov/sites/default/files/uploads/agreements/fta/korus/asset_upload_file816_12714.pdf

[32] Article 13.11 in the First Amendment to the Additional Protocol to the Framework Agreement of the Pacific Alliance available in Spanish at https://alianzapacifico.net/download/primer-protocolo-modificatorio-del-protocolo-adicional-al-acuerdo-marco-de-la-alianza-del-pacifico/

[33] Ibid

[34] Article 13.11 of Peru Australia FTA (PAFTA) https://dfat.gov.au/trade/agreements/not-yet-in-force/pafta/Pages/peru-australia-fta.aspx

[35] Article 13.2 PAFTA

[36] Chapter 28 PAFTA

United States, Mexico and Canada Agreement (USMCA)

The agreement among United States of America, Mexico, and Canada which is supposed to supersede NAFTA has been signed but not yet ratified.

In slightly different language from the agreements above, this agreement also calls for no prohibition or restriction on transfer of information across borders, barring legitimate public policy objectives that are not arbitrary or disguised restrictions on trade. Additionally, it explains in a footnote that, if an imposed measure alters the conditions of competition to the detriment of a service provider, that measure would be in violation to the provision[37]. The agreement clarifies in its scope that there are separate rules to address data transfer obligations with respect to financial service suppliers[38].

A similar rule covers locating computing facilities but without the public policy caveat[39]. It also mentions that separate rules apply to data localization obligations with respect to financial service suppliers.

[37] Article 19.11 of USMCA https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19_Digital_Trade.pdf

[38] Article 19.2

[39] Article 19.12

SECTION 3

Regulatory Issues concerning Technology and Source Code

Apart from data, source code has arisen as an issue of much attention. The debate surrounding source code deals with the wider discussions on acquisition of digital technologies and capabilities and also borders on the realms of intellectual property laws.

3.1 Understanding the Concept

Source code can be defined as a collection of instructions typed into a computer which are processed and executed to enable some actions by the computer. It forms the fundamental component of a computer programme, something responsible for driving the software, and can be easily read and understood by a human being. In fact, it is the human-readable version of the programme which is specifically called the source code, as opposed to the object code which is the computer readable component of the same programme which is eventually executed[40].

Developing a source code is creative work within the data industry. That is why among computer programmers, sharing and reviewing existing source code helps to acquire newer programming techniques. By working with and developing new source code, programmers become more mature in handling the complex techniques. The quality of the source code also determines the performance of the software, in its ability to cater for updates and debugging during its use.

Nowadays, the source code is usually kept confidential to protect proprietary information and can often protected by copyright. During the early phases of the digital revolution, when home computers and digital devices were first introduced, source code was not protected by intellectual property laws. Software was considered as public domain and used openly. During the 1970s and 1980s, computer programmes were made copyrightable as literary work since they constituted 'authorship'. With the evolution of IP protection surrounding source code, two kinds of software are generally recognised, i.e. copyrighted and open-source. In general, if the source code is free to use, study, distribute, or modify, the software is called open-source. Similarly, it is considered proprietary if the source code is kept secret, or is privately owned or restricted.

3.2 The Debate Surrounding Source Code

With the emerging significance of digital technology, the importance of information contained in source codes has gained vast importance. It can be argued that the source code, algorithms, and encryption techniques embody the technology that drives the digital

[40]Lin, D. S., Sag, M., and R. S. Laurie, "Source Code versus Object Code: Patent Implications for the Open Source Community", Santa Clara High Tech. Law Journal, 18,235, 2002, http://digitalcommons.law.scu.edu/chtlj/vol18/iss2/3

innovation of the modern day, and are considered useful assets. Large companies that develop software jealously guard this information as their intellectual property, much like patents and layout designs in the conventional industrial sector. Countries where such large companies are located and hold power, often lobby for protection of source code information as trade secrets. Recent trade agreements have incorporated such provisions as will be discussed later in this section.

In fact, large companies and advanced countries have argued that requirements in other countries demanding local partnership or transfer of technology, access to encryption keys, disclosure of source code and algorithms are all burdensome market access barriers that restrict the ability of these companies to operate in foreign markets. These barriers, thus, force companies to abandon key foreign markets. Countries that are potential recipients of such businesses are often advised that they should not erect such barriers in their investment policies as they can dissuade investors.

On the other side, for countries that are still backward in digital technology, there could be various reasons for requiring access to source code. Access to programming information, data analytics and other techniques is considered a vital cog in their development of the required digital kills. Restricting access to source code would therefore, be seen as preventing transfer of crucial technology. Since 'compatibility' in the digital world is of prime significance, the mere functional description of a computer programme is not sufficient for programmers to replicate. Software is only useful depending on the platform or operating system on which it functions. Since most platforms and their programming interface is also kept secret, it is virtually impossible for third party application or software providers to develop sophisticated computer applications [41].

Increasingly, as manufacturing and production techniques are digitalised at great pace, access to digital technology in the form of source code could be seen as extremely important in order to keep up with modern industrial standards. With the advent of robots, artificial intelligence and 3-D printing, more and more products now contain software which is difficult to produce or replicate without source code.[42]

Countries may also demand source code to reign in anticompetitive conduct of companies. If a company has been found to violate competition laws, they could be required to transfer source code (or products/services/technology containing the source code) to competitors as a remedy[43] . In addition, governments could use source code to implement anti-discrimination policies, product safety standards (such as for automobiles), regulate financial and stock markets, provide protection against cybercrime (including cyber threats to national security) and a host of other policy objectives to protect human health and security.

Access to a company's source code makes it very easy to detect security flaws and vulnerabilities for surveillance and intelligence-gathering operations. This has been used often in the United States. There is, therefore, also an argument that while source code is a trade secret and its disclosure should not be mandatory in any law, allowance should be made for legitimate objectives such as national security.

Together with data localisation discussed above, source code sharing also forms part of the larger

[41] Tomkowicz, R., "Intellectual Property Overlaps: Theory, Strategies and Solutions", Routledge, 2013.

[42] Kelsey 2017, see note 17.

[43] Ibid 42; Smith, S. R., "Some Preliminary Implications of WTO Source Code Proposal", Third World Network (TWN) Briefings 4, 2017,

discussion on transfer of technology and mandatory performance requirements for investors and service providers. Along with source code, other information such as encryption keys and algorithms can also be demanded by governments as a condition for companies locating their businesses or business operators providing their services in their countries. Other conditions can include the requirement to form local partnerships (otherwise known as joint-ventures) and development of local data centres using technology made available to partner forms[44].

Such performance and technology transfer requirements are not new in the trading world. It is only that they are now being applied in the same way to digital trade as they did to conventional trade. The WTO's TRIMs agreement was designed to address similar policies and has attracted similar debate over the years, with developed countries generally supporting no performance requirements and developing countries seeking higher technology, favouring the need for such domestic laws or policies.

Nevertheless, several countries across the world have in the past, and also currently use such policies. These can either be specifically aimed at sharing or disclosing source codes or any other measure, or could be used in combination with other requirements for technology transfer. Since the subject is fairly new, only a few specific examples of policies aimed at source code disclosure can be found. It is expected that countries may develop more regulations with the passage of time and as their understanding of the issues becomes more profound. Some country examples of such measures are discussed below:

3.3 National Policies for Source Code Disclosure

China

Although recently suspended, a notice from the China Banking Regulatory Commission (CBRC) had a requirement to make at least 75% technology supplied to Chinese banks "safe and controllable" by 2019. Firms were mandated to disclose the source code of the software and firmware supplied to Chinese banks to ensure the implementation of this safety clause[45].

The notice was revised under the new Cybersecurity Law which contains provisions requiring tech companies to provide unspecified "technical support" to security agencies, which potentially includes source code sharing. The new law is softer in its requirement but does speak to the need for source code sharing for reasons of safety and security.

Indonesia

Service providers developing any software for a government agency are required under Indonesian law to submit the source code and documentation of the software concerned either to the government agency itself or to a third party under the Regulation n. 82 of 2012[46].

[44] United States Information Technology Office (USITO), "Written Comments to the U.S. Government Interagency Trade Policy Staff Committee in Response to Federal Register Notice Regarding China's Compliance with its Accession Commitments to the World Trade Organization (WTO)", 20 September 2013.

[45] Bird, R. and J.K. Warren, "China introduces comprehensive new cyber security rules for banking procurement", Briefing Note, Freshfields Bruckhaus, Deringer, March 2016.

[46] Article 8, "Regulation Number 82 of 2012 Concerning Electronic System and Transaction Operation", Government of the Republic of Indonesia, 2012 http://www.flevin.com/id/lgso/translations/JICA%20Mirror/english/4902_PP_82_2012_e.html

Nigeria

Nigeria has maintained elaborate performance requirements including those on local content and technology transfer. The Oil and Gas Industry Content Development Act of Nigeria promotes transfer of technology between firms and requires disclosure of confidential information to the Nigerian Content Development and Monitoring Board (NCDMB). As part of these larger performance and localisation requirements in Nigeria, source code disclosure to government ministries, departments and agencies is also required.[47]

Russia

The Russian Federation has recently suggested that Apple, and similar companies should disclose their source code to fulfil security related conditions, for example, that the software will not be used to spy on Russian citizens[48]. It has also been reported that large software enterprises such as SAP, Symantec and McAfee allowed the Russian government to examine their source codes for vulnerabilities as a precondition to entering the Russian market[49].

Brazil[50]

Brazil has been an advocate of using open source software for several years. In 2014, in attempt to maintain cyber-security, an Inter-Ministerial Ordinance (141/2014) was published by the government. The ordinance mandates that IT equipment sold to government institutions and public enterprises must be certified to be clear of security threats and backdoors. Companies must make it possible to of audit programmes and equipment in order to fulfil these requirements. This requires "opening the source code in the case of programs for data communication and firmware and operating systems in the case of data communication equipment".[51]

South Africa

The government of South Africa, since 2006, implements a Free and Open Source Software (FOSS) policy[52] for all government departments and agencies. According to the policy, any new software developed for or by the government for any project must be FOSS, unless proprietary software is demonstrated to be considerably superior. Moreover, it mandates migration from all existing proprietary software to open source software.

Essentially, such requirements mean that the government allows only open source software to be used. Companies providing proprietary software only have the choice of making their product open source, i.e. disclose the source code, to be able to supply their software. It, therefore, works as an indirect source code disclosure requirement.

India

Similar to South Africa, the government of India, in 2013, announced a "Policy on Adoption of Open Source Software for Government of India"

---

[47] Ibid 45; Federal Ministry of Communications Technology, "Guidelines for Nigerian Content Development in Information and Communications Technology 2013", Government of Nigeria, https://nlipw.com/wp-content/uploads/Guidelines-for-Nigerian-Content-Development-in-Information-and-Communications-Technology-ICT.pdf

[48] Ibid 45;

[49] Blackmon, K., "Why Partners Should Care About Russian Mandatory Source Code Reviews", Chanel Futures, February 13, 2018, https://www.channelfutures.com/strategy/why-partners-should-care-about-russian-mandatory-source-code-reviews

[50] Neeraj, 2017.

[51] Chapter V, Article 14 of Inter-Ministerial Ordinance MP/MC/MD Nº141 of 05/02/2014, https://www.legisweb.com.br/legislacao/?id=269793

[52] Department of Public Service & Administration, "Policy on Free and Open Source Software Use for South African Government", 2006, http://unpan1.un.org/intradoc/groups/public/documents/cpsi/unpan025432.pdf

as part of its 'Digital India Programme'. This policy requires that Open Source Software (OSS) be installed in all e-Governance systems implemented by various central and state level government departments, as a preferred option in comparison to proprietary software. It is mandated that suppliers to the government provide justification for exclusion of OSS in their response to procurement calls. The final decision must be made based on "capability, strategic control, scalability, security, life-time costs and support requirements."[53]

Such a condition would work in the same way as in the case of South Africa, by ensuring that proprietary software is only used once the source code is disclosed.

3.4 Provisions in Trade Agreements Covering Source Code and Technology Transfer

At the international level, some countries have signed RTAs prohibiting performance requirements related to technology transfer including source code requirements. Some technology transfer conditions are also covered in Bilateral Investment Treaties but they do not deal with source codes explicitly. The issue is also one under discussion at the joint statement initiative on E-Commerce at the WTO where some members are proposing the addition of these provisions in the final agreement on E-Commerce.

In general, the RTAs contain provisions that parties do not require the transfer of, or access to, source code of software owned by a person of the other Party, as a condition for the import, distribution, sale or use of such software, or of products containing such software. Some examples are illustrated below:

Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)

The agreement stipulates that no Party shall require the transfer of, or access to, source code of software owned by a person of another Party, as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory[54].

It further clarifies that the term 'software' is limited to mass-market software or products containing such software and does not include software used for critical infrastructure.

Another provision allows the inclusion or implementation of terms and conditions related to the provision of source code in commercially negotiated contracts; and also, allows a Party to require the modification of source code of software necessary for that software to comply with laws or regulations which are not inconsistent with the RTA in general.

Lastly, the agreement stipulates that the provision on source code cannot be construed to affect requirements that relate to patent applications or granted patents, or any judicial orders in patent disputes.

In addition to source code requirements, the CPTPP also covers extensively issues related to technology transfer, cryptography and local partnership[55]. The agreement lays down that no

[53] F. No. 1(3)/2014 – EG II, Ministry of Communication & Information Technology Department of Electronics & Information Technology, Government of India http://meity.gov.in/sites/upload_files/dit/files/policy_on_adoption_of_oss.pdf

[54] Article 14.17

[55] Annex 8-B

Party can impose or maintain a technical regulation or conformity assessment procedure that requires a manufacturer or supplier of the product, as a condition of the manufacture, sale, distribution, import or use of the product, to transfer or provide access to a particular technology, production process, a private key or other secret parameter, algorithm specification or design detail, that is proprietary to the manufacturer or supplier and relates to the cryptography in the product.

It further requires that there can be no requirement by a country for a business to partner with a person in its territory; or to use or integrate a particular cryptographic algorithm or cipher, other than where the manufacture, sale, distribution, import or use of the product is by or for the government of the Party.

EU-Mexico FTA[56]

This FTA prohibits parties from requiring the transfer of, or access to, source code of software owned by a juridical or natural person of the other Party. However, parties may do so to achieve a legitimate public policy objective, including to ensure security and safety[57].

Parties are also allowed to voluntarily transfer or grant access to source code on a commercial basis by a person of the other Party, for instance in the context of a public procurement transaction or a freely negotiated contract[58].

A further caveat provides that the provisions on source code do not affect requirements by a court, administrative tribunal or competition authority to remedy a violation of competition laws; intellectual property rights and their enforcement; and the right of a Party to take any action or not disclose any information that it considers necessary for the protection of its essential security interests such as procurement of arms, ammunition or war materials[59].

Japan-EU EPA[60]

Similar to the Mexico-EU FTA, this agreement also prohibits parties from requiring the transfer of, or access to, source code with the caveats that it may be done in commercially negotiated contracts, or on a voluntary basis, for instance in the context of government procurement. The agreement also clarifies that source code includes source code of software contained in a product[61].

Further provisions allow courts or administrative tribunals the authority to require source code disclosures to remedy a violation of competition law or for the protection and enforcement of intellectual property rights and in accordance with the Government Procurement Agreement.[62]

United States, Mexico and Canada Agreement (USMCA)

The USMCA covers the subject of source code, technology transfer requirements and encryption technologies in much detail.

On the issue of source code, it mandates that no Party can require the transfer of, or access to, source code of software owned by a person of

[56] The agreement has been recently negotiated and the legal text is subject to revision (European Commission, http://ec.europa.eu/trade/policy/countries-and-regions/countries/mexico/ accessed 21 January 2019).

[57] Chapter 16, Article 9, http://trade.ec.europa.eu/doclib/docs/2018/april/tradoc_156811.pdf accessed 21 January 2019

[58] Ibid.

[59] Ibid.

[60] The agreement has been recently concluded and is expected to enter into force on 1st February 2019 (European Commission, http://ec.europa.eu/trade/policy/in-focus/eu-japan-economic-partnership-agreement/ accessed 21 January 2019)

[61] Article 8.73, http://trade.ec.europa.eu/doclib/docs/2018/august/tradoc_157228.pdf#page=185 accessed 21 January 2019.

[62] Ibid.

another Party, or to an algorithm expressed in that source code, as a condition for the import, distribution, sale or use of that software, or of products containing that software, in its territory.

It does, however, allows for disclosure to only judicial authorities for a specific investigation, inspection, examination enforcement action or judicial proceeding, subject to safeguards against unauthorized disclosure[63].

On technology transfer, the agreement specifies that no Party can impose or enforce any requirement, or enforce any commitment or undertaking in connection with the establishment, acquisition, expansion, management, conduct, operation, or sale of an investment in its territory, or to require the investor to transfer a technology, a production process or other proprietary knowledge to a person in its territory[64].

A similar treatment is granted to encryption methods[65]. No party to the agreement can require a manufacturer or supplier of the good, as a condition of the manufacture, sale, distribution, import, or use of the good, to transfer or provide access to any proprietary information relating to cryptography, including by disclosing a particular technology or production process, a private key or other secret parameter, algorithm specification, or other design detail. Further, no party can place a requirement on companies to partner or otherwise cooperate with a person in its territory in the development, manufacture, sale, distribution, import, or use.

This provision, however, eliminates from its application law enforcement authorities requiring service suppliers using encryption they control to provide unencrypted communications, and the regulation of financial instruments, networks of central banks, or measures taken pursuant to supervisory, investigatory, or examination authority relating to financial institutions or financial markets.

[63] Article 19.16
[64] Article 14.10
[65] Article 12.C.2

SECTION 4

Discussion and Conclusions

The evolution of the digital economy has enabled superior production methods, created more efficiency in the conduct of business, and thrown up tremendous opportunities for countries to develop their economies at a greater pace. At the same time, it has unravelled new and complex concepts, requiring much higher levels of technical know-how and technological capabilities to effectively make use of the innovations.

While the modes and methods of economic transactions stand revolutionised in this digital trade environment, issues surrounding trade and international political economy appear to remain the same. As with conventional trade in goods and services, it is the ownership of resources and command over technology that not only differentiates countries across the trading map, but also forms the contours of debate on international trade.

Rapid advancements in digital technology and E-Commerce have opened new vistas for countries to expand businesses, but their ability to do so is constrained by the stark digital divide. The divide represents not only the wide-ranging differences in infrastructure between technologically advanced and poorer countries, but also highlights the information or knowledge gap, and the large variance in technological skills and capabilities between these sets of countries. The divide is a new phenomenon only in that it is digital. In earlier times, it pointed to the gap in industrial capabilities and production capacities.

It is understandable then, that issues surrounding international digital trade and commerce would pivot around similar points as those with conventional trade in goods and services. The brief analysis above has revealed that issues surrounding data flows, data localisation, source code sharing and technology transfers are debated between removal of restrictions and barriers to E-Commerce across the globe on the one hand and attempts by countries to harness new technologies and develop local skills and capacities on the other.

International rules on such issues, both multilateral and in RTAs, have existed in the form of prohibitions on technology transfer policies and local content requirements, protection for proprietary knowledge, and disciplines on restrictions to flow of trade. The TRIMs and TRIPS agreements with some GATT and GATS obligations are good examples. Such agreements have received equal criticism and appreciation from respective quarters.

Thus, many countries today employ policies that regulate the flow of data and mandate its storage on local servers. Many larger developing countries such as India, China, Russia, Turkey etc. that are attempting to evolve their digital infrastructure and capabilities are seen using such policies which can take various shapes. Smaller developing countries are still in a phase of developing their digital policies, though there are visible attempts as in the case of Rwanda.

Similarly, a few countries have attempted to use various forms of technology transfer requirements such as source code disclosure, or mandatory partnerships with local firms and sharing of encryption keys. Evidence has been found in cases like Nigeria, Russia, China, India, South

Africa and some others that may have relinquished such policies.

On the other hand, developed countries have called such policies as protectionist and restrictive for the flows of trade and harmful for their tech companies that seek to invest abroad. They argue that localisation and data flow restrictions increase the cost of digital transactions and erect barriers to trade which can be harmful for both developed and developing countries. They also refer to technology transfer provisions as forced requirements to share knowledge which is otherwise secret or protected under IP laws.

In order to restrict the use of such policies by others, countries have resorted to regional trade agreements that clearly specify that these restrictions cannot be used as a condition to conduct business. Some of these agreements make allowances for such policies in the case of legitimate public policy objectives, such as to protect life, health or national security. In case of source codes and encryption technologies, allowances have also been made in these RTAs for judicial proceedings under competition or IP laws.

It is also argued that the new advancements in the digital age are not covered under current WTO agreements. Therefore, attempts have been made at framing new multilateral rules on E-Commerce. While such attempts were blocked by several developing countries in the lead up to MC-11, like-minded countries had signed a joint statement to initiate discussions among themselves for possible negotiations on a new agreement. Formal negotiations among these countries may commence sometime in 2019. Those that oppose this initiative call such negotiations too early for developing countries who find themselves at much lower levels of digital development.

The debate is unlikely to be settled very soon. Prima facie, the calls for removing barriers to trade and allow for all countries to gain from expansion in E-Commerce and digital trade may seem plausible. At the same time, the need for developing countries to scale up their infrastructure, develop requisite skills and capacities and acquire modern technologies is also genuine. Recent studies by UNCTAD[66] have argued that, for developing countries, among other policies, South-South cooperation and investment in digital infrastructure may be the way forward. Regional cooperation among countries with similar levels of development may allow them to learn quickly from each other and develop requisite skills to compete globally.

In the end, it would be up to each individual country to assess its level of development, its own socio-economic requirements and capabilities to enact policies in line with its national development objectives and policies while remaining cognizant of its obligations under the relevant regional and multilateral agreements and the needs of discussions/negotiations in these fora.

[66] Ibid 14; UNCTAD, "South-South Digital Cooperation for Industrialization: A Regional Integration Agenda" 2018, https://unctad.org/en/PublicationsLibrary/gdsecidc2018d1_en.pdf

References

Bird, R. and J.K. Warren (2016), "China Introduces Comprehensive New Cyber Security Rules for Banking Procurement", Briefing Note, Freshfields Bruckhaus, Deringer, March 2016 http://knowledge.freshfields.com/m/Global/r/1514/china_introduces_comprehensive_new_cyber_security_rules

Blackmon, K. (2018), "Why Partners Should Care About Russian Mandatory Source Code Reviews", Chanel Futures, February 13, 2018, https://www.channelfutures.com/strategy/why-partners-should-care-about-russian-mandatory-source-code-reviews

City of Los Angeles, Office of the City Clerk (2009), "City of Los Angeles: Supplemental Report – Information Technology Agency Request to Enter into a Contract with Computer Science Corporation for the Replacement of the City's Email System," http://clkrep.lacity.org/onlinedocs/2009/09-1714_rpt_cao_10-7-09.pdf

Cory, N (2017), "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" Information Technology and Innovation Foundation (ITIF), May 1, 2017.

Department of Foreign Affairs and Trade, Australia, "Peru Australia Free Trade Agreement (PAFTA)", https://dfat.gov.au/trade/agreements/not-yet-in-force/pafta/Pages/peru-australia-fta.aspx

Eggers, W.D., Hamill, R. and A. Ali (2013), "Data as the New Currency - Government's Role in Facilitating the Exchange", Deloitte Review, Issue 13

European Commission, EU-Japan Economic Partnership Agreement, http://ec.europa.eu/trade/policy/in-focus/eu-japan-economic-partnership-agreement/

European Commission, EU-Mexico Free Trade Agreement, http://ec.europa.eu/trade/policy/countries-and-regions/countries/mexico/

GIZ (2017), "Data for development: What's next? Concepts, Trends and Recommendations for German Development Cooperation", Deutsche Gesellschaft für Internationale Zusammenarbeit

Government of Brazil (2014), Inter-Ministerial Ordinance MP/MC/MD Nº141 of 05/02/2014, https://www.legisweb.com.br/legislacao/?id=269793

Government of India (2013), "Policy on Adoption of Open Source Software for Government of India", Ministry of Communication & Information Technology Department of Electronics & Information Technology, http://meity.gov.in/sites/upload_files/dit/files/policy_on_adoption_of_oss.pdf

Government of Indonesia (2012), “Regulation Number 82 of 2012 Concerning Electronic System and Transaction Operation”
http://www.flevin.com/id/lgso/translations/JICA%20Mirror/english/4902_PP_82_2012_e.html

Government of Nigeria (2013), “Guidelines for Nigerian Content Development in Information and Communications Technology 2013”, Federal Ministry of Communications Technology, https://nlipw.com/wp-content/uploads/Guidelines-for-Nigerian-Content-Development-in-Information-and-Communications-Technology-ICT.pdf

Government of Rwanda, “Data Revolution Policy” National Institute of Statistics of http://statistics.gov.rw/publication/rwanda-national-data-revolution-and-big-data

Government of South Africa (2006), “Policy on Free and Open Source Software Use for South African Government”, Department of Public Service & Administration, http://unpan1.un.org/intradoc/groups/public/documents/cpsi/unpan025432.pdf

Government of South Korea (2014), “Act on the Establishment, Management, etc. of Spatial Data”, Ministry of Land, Infrastructure and Transport, http://elaw.klri.re.kr/eng_service/lawView.do?hseq=32771&lang=ENG.

Kelsey, J. (2017), “The Risks for ASEAN of New Mega-Agreements that Promote the Wrong Model of E-Commerce”, ERIA Discussion Paper Series, https://think-asia.org/bitstream/handle/11540/7662/ERIA-DP-2017-10.pdf?sequence=1

Lin, D. S., Sag, M., and R. S. Laurie (2002), “Source Code versus Object Code: Patent Implications for the Open Source Community”, Santa Clara High Tech. Law Journal, 18, 235 http://digitalcommons.law.scu.edu/chtlj/vol18/iss2/3

Meltzer, J. (2015), “A New Digital Trade Agenda”, E15 Initiative 2

Ministry of Foreign Affairs and Trade, New Zealand, “Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)”, https://www.mfat.govt.nz/assets/Trans-Pacific-Partnership/Text/14.-Electronic-Commerce-Chapter.pdf

Neeraj, R.S. (2017), “Trade Rules on Source Code-Deepening the Digital Inequities by Locking Up the Software Fortress” Working Paper CWS/WP/200/37, Centre for WTO Studies, Indian Institute of Foreign Trade

OECD (2016), “The Economic Impact of Local Content Requirements “Trade Policy Note, https://www.oecd.org/tad/policynotes/economic-impact-local-content-requirements.pdf.

OECD (2017), “International Technology Transfer Measures in an Interconnected World: Lessons And Policy Implications”, Trade and Agriculture Directorate, TAD/TC/WP(2017)1/FINAL

Pacific Alliance, Framework Agreement of the Pacific Alliance, First Amendment to the Additional Protocol https://alianzapacifico.net/download/primer-protocolo-modificatorio-del-protocolo-adicional-al-acuerdo-marco-de-la-alianza-del-pacifico/

Parkins, D. (2017), "The World's Most Valuable Resource", The Economist, 6 May

Sacks, S. (2018), "China's Emerging Data Privacy System and GDPR", Centre for Strategic and International Studies (CSIS)

Sen, N. (2018), "Understanding the Role of the WTO in International Data Flows: Taking the Liberalization or the Regulatory Autonomy Path?" Journal of International Economic Law, Vol 21, Issue 2, 323–348.

Smith, S. R. (2017), "Some Preliminary Implications of WTO Source Code Proposal", Third World Network (TWN) Briefings 4

Tarnoff B. (2018), "Big data for the people: It's time to take it back from our tech overlords", The Guardian, 14th March

Tomkowicz, R., (2013), "Intellectual Property Overlaps: Theory, Strategies and Solutions", Routledge

U.S. Department of Defense (2015), "Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018)", Washington DC, https://www.federalregister.gov/documents/2015/08/26/2015-20870/defense-federal-acquisitionregulation-supplement-network-penetration-reporting-and-contracting-for

U.S. Internal Revenue Service (2016), "Publication 1075: Tax Information Security Guidelines for Federal, State and Local Agencies", Washington, DC, https://www.irs.gov/pub/irs-pdf/p1075.pdf

UNCTAD (2017), Information Economy Report

UNCTAD (2018), "South-South Digital Cooperation for Industrialization: A Regional Integration Agenda", https://unctad.org/en/PublicationsLibrary/gdsecidc2018d1_en.pdf

UNCTAD (2018), Trade and Development Report

United States Information Technology Office (USITO) (2013), "Written Comments to the U.S. Government Interagency Trade Policy Staff Committee in Response to Federal Register Notice Regarding China's Compliance with its Accession Commitments to the World Trade Organization (WTO)"

United States Trade Representative (USTR), Korea-United States Free Trade Agreement, https://ustr.gov/sites/default/files/uploads/agreements/fta/korus/asset_upload_file816_12714.pdf

United States Trade Representative (USTR), United States, Mexico and Canada Agreement (USMCA), https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19_Digital_Trade.pdf

van der Marel, E. (2015), “Disentangling the Flows of Data: Inside or Outside the Multinational Company”, European Centre for International Political Economy (ECIPE), Occasional Paper, 7

WTO (1998), “Declaration on Global Electronic Commerce” (25 May 1998) WT/MIN(98)/DEC/2

WTO (1998), “Work Programme on E-Commerce” WT/L/274

WTO (2017), Joint Statement on E-Commerce (13 December 2017) WT/MIN(17)/60