What has Digital Trade Brought to Trade Agreements? — Focusing on Non-trade Concerns *

IINO Aya

Professor, Faculty of Commerce, Nihon University

Abstract

The growing digitalization in the economy and society has brought a variety of impacts and new challenges for international trade. As a result, there is a need for changes or evolutions in trade agreements to adapt to this trend. Shedding light on some of these emerging changes or evolutions in trade agreements, this paper aims to examine the emerging global regulatory environment for digital trade, particularly in Free Trade Agreements (FTAs).

To that end, it first provides an overview of the concepts of digital trade and reviews the key impacts and challenges arising from the growth of digital trade. It then examines the extent to which trade agreements are adapting to these challenges by analyzing World Trade Organization (WTO) agreements and FTAs. The FTAs considered here are the advanced FTAs of the "rule-maker" countries that are leading the way in establishing digital trade rules, namely CPTPP, USMCA, DEPA, DEA, UKSDEA, EU-UKTCA, and EUSDTP. In addition, RCEP is also included in the scope, as it covers major trading partners.

Based on the results of the research, the paper presents the following conclusions: firstly, the state of mutual interaction between agreements in the formation of digital trade rules; secondly, the extension of the reach of trade agreements brought about by digital trade and the implications thereof; thirdly, the increasing presence of the "right to regulate" in trade agreements in consonance with the emergence of digital trade rules; and fourthly, the need for increased stakeholder participation in the regulation of digital trade.

Keywords: digital trade, electronic commerce (e-commerce), cross-border data transfer, cybersecurity, personal information protection, WTO, FTA, right to regulate

JEL Classification: F13, F15, K33

* The author would like to express thanks for all questions and comments made during the research group meetings held by the Policy Research Institute, Ministry of Finance Japan.

The Japanese version of the paper has been updated and supplemented in this English version in light of the subsequent developments, including the progress of the negotiations. This includes IV-2 and its footnotes, as well as footnotes 39, 40, 50, 96, 102, 128, 133, 171.

I. Introduction

The growing digitalization in the economy and society has brought a variety of impacts and new challenges for international trade. In particular, data,[1] the transaction volume of which has increased with technological progress, is itself transacted, closely linked to the means of providing services (e.g. SNS, online games), and also a means of promoting the development of new services (e.g. cloud computing, generative Artificial Intelligence (AI)). As a new value generator in this way, data also affects the sources of comparative advantage between nations. As a result, new trade barriers such as data-related measures have emerged, as well as the need to ensure the protection of personal data and cybersecurity over data transferred across borders. Furthermore, while data is transferred across national borders, regulations in each country are administered on a country-by-country basis, so regulatory differences between countries have led to higher costs and increased legal instability for business, and tensions between countries. Against this background, there is a need for trade agreements to change or evolve to address these challenges.

Shedding light on some of these changes or evolutions in trade agreements, this paper aims to examine the emerging global regulatory environment for digital trade, particularly in Free Trade Agreements (FTAs).[2] Following this introduction, Section II first provides an overview of the concepts of digital trade, and Section III reviews the key impacts and challenges on trade arising from the growth of digital trade. It then examines the extent to which trade agreements are adapting to these challenges, starting with an analysis of World Trade Organization (WTO) agreements in Section IV. Section V then focuses mainly on the advanced FTAs of the "rule makers," the countries that are leading the way in establishing digital trade rules. Finally, Section VI presents the conclusions.

II. What is Digital Trade?

This section explores the concept of digital trade by looking at some examples of how digital trade is currently perceived by key trade-related international organisations, researchers and countries.

According to the Organisation for Economic Co-operation and Development (OECD), "(w)hile there is no single recognised and accepted definition of digital trade, there is a growing consensus that it encompasses digitally-enabled transactions of trade in goods and ser-

[1] In this paper, the terms "data" and "information" are used interchangeably, given that each is not defined in the FTAs examined in this paper.

[2] For the sake of simplicity, this paper refers to free trade agreements and customs unions, which GATT Article XXIV distinguishes, and other trade agreements that do not necessarily cover market access commitments, collectively as free trade agreements (FTAs), unless otherwise noted.

vices that can either be digitally or physically delivered, and that involve consumers, firms, and governments" and "(u)nderpinning digital trade is the movement of data" that is not only a means of production, but also an asset that can itself be transacted.[3] In the WTO context, the concept of electronic commerce (e-commerce), as set out in the WTO Work Programme on Electronic Commerce,[4] is well recognised, being understood, exclusively for the purposes of the Work Programme, as "the production, distribution, marketing, sale or delivery of goods and services by electronic means."[5] Recently, the International Monetary Fund (IMF), OECD, the United Nations (UN) and WTO jointly developed for the first time a statistical definition of digital trade as "all international trade that is digitally ordered and/or digitally delivered."[6]

Among the commentators, Peng (2022) states that "there is no single recognized and accepted definition of digital trade...(it) is generally understood in a broad sense that encompasses international trade enabled by digital technologies…The term 'digital trade' is often used interchangeably with terms such as 'e-commerce' or 'trade aspects of e-commerce.'"[7]

The key FTAs with provisions on digital trade rarely include a definition of digital trade or e-commerce, but some references can be found on the websites of the countries concerned. The EU describes that "(d)igital trade refers to commerce enabled by electronic means—by telecommunications and/or Information and Communication Technology (ICT) services—and covers trade in both goods and services."[8] Australia, in its "Digital Trade Strategy" and for the purpose of this strategy, considers digital trade as including: 1) imports and exports of goods sold over the Internet and e-commerce platforms, digital content (software, books, music, films, apps, etc.) and digitally-enabled services (legal, financial, education, consultancy, etc.); 2) electronic facilitation of trade, such as the acceptance of electronic trade documents and, possibly, the adoption of "regtech" solutions as technology evolves; and 3) the transmission of data across borders as a business activity in its own right and to support other business activities.[9] New Zealand states that while there is no single accepted definition of digital trade, a growing consensus has been observed on the above stated OECD definition, and describes

---

[3] OECD <https://www.oecd-ilibrary.org/trade/digital-trade_524c8c83-en> This concept was first introduced by Gonzalez and Jouanjean (2017) OECD Trade Policy Papers González and Jouanjean (2017), pp. 7, 12.

[4] WTO, WT/L/274, 30 September 1998.

[5] In the WTO EC-JSI negotiations, this "definition" seemed to be referred to as the definition of digital trade and/or e-commerce in the draft text. Peng (2022) p. 772, ft.9. In the World Trade Report, annual publication of the WTO, has referred the definition of the OECD, while stating that there is no agreed definition on digital trade. WTO (2018) Section B, ft.21.

[6] IMF, OECD, UN and WTO (2023) p. 5. "Digitally ordered trade" is defined as "the international sale or purchase of a good or service, conducted over computer networks by methods specifically designed for the purpose of receiving or placing orders," and "digitally delivered trade" is defined as "all international trade transactions that are delivered remotely over computer networks." Ibid., p. 6.

[7] Peng (2022) pp. 772-773.

[8] EU, "Digital trade" <https://policy.trade.ec.europa.eu/help-exporters-and-importers/accessing-markets/goods-and-services/digital-trade_en>

[9] Australian Government, Department of Foreign Affairs and Trade, "Digital Trade Strategy" <https://www.dfat.gov.au/trade/services-and-digital-trade/e-commerce-and-digital-trade/digital-trade-strategy>

digital trade as "anything that is enabled by digital technologies whether or not it is digitally or physically delivered...(including) the purchase and physical delivery of a paper book through an on-line marketplace as well as the purchase and digital delivery of an e-book." It further describes that "digital trade" and " e-commerce" are often used interchangeably.[10]

While the above represents only part of the picture, some commonalities can be found: first, digital trade is a broad concept that has no universally accepted definition but encompasses digitally tradable goods and services, whether delivered digitally or physically; second, digital trade is underpinned by data; and third, digital trade is often used interchangeably with e-commerce.

On this basis, if the current common understanding of digital trade is summarised, it can encompass at least digitally enabled international trade in goods and services, including physically deliverable goods, and cross-border trade in data itself, which is underpinned by data. In any case, given the speed of technological innovation, the scope of digital trade is likely to change accordingly. As for the relationship between digital trade and e-commerce, although digital trade seems to encompass international e-commerce,[11] as shown, for example by the comparison between the WTO's understanding on e-commerce and Australia's definition of digital trade, digital trade and e-commerce are used interchangeably in this paper for the time being.

III. Implications and Challenges for International Trade

What are the implications and challenges of digital trade for international trade? As discussed in the previous section, digital trade is underpinned by data, and data itself is transacted.[12] The importance of data is that it changes the sources of comparative advantage, or "competitiveness," of countries, and the infrastructure that ensures the flow of data is also part of the sources of comparative advantage.[13] On this point, further technological development is envisioned for large capacity networks, the main infrastructure for data flow, including the spread of 5G, the development of satellite Internet,[14] the development of space laser communication,[15] attempts to lay submarine cables in the Arctic,[16] and the possible deployment of quantum communication technology, among

[10] New Zealand Government, Foreign Affairs and Trade, "What is 'the digital economy' and 'digital trade'?" <https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement-depa/what-is-the-digital-economy-and-digital-trade>

[11] The conceptual differences between digital trade and e-commerce are well explained in IMF, OECD, UN and WTO (2023) Figure 1.4. IMF, OECD, UN WTO (2023), p. 14

[12] Indeed, according to the McKinsey Global Institute (2016), of the global flows of goods, foreign direct investment and data contributing to the development of world GDP, already in 2014, the contribution of global data flows exceeded that of trade in goods. McKinsey Global Institute (2016), pp. 75, 77.

[13] This is reflected in the phrase "data is the new oil." See The Economist (May 6, 2017). The WTO notes that, in 2018, regulation of intellectual property rights, data flows, and privacy as well as the quality of digital infrastructure are likely to emerge as new sources of comparative advantage. WTO (2018), p. 63.

[14] E.g., Starlink announced on Twitter (now X) that it became the first company in Asia to start supplying services in Japan in October 2022. The Asahi Shimbun (October 11, 2022) and The Nikkan Kogyo Shimbun (November 23, 2022).

[15] REUTERS (June 3, 2022).

[16] REUTERS (December 2, 2022).

others. The growth trend of the Internet population in the past suggests that it will continue to grow in the future.[17] These developments are expected to further deepen the significance of data and the shifts in sources of comparative advantage.

Due to these changes in the sources of "competitiveness," the main challenges facing international trade are as follows. Firstly, new trade restrictive measures have emerged. As the importance of data grows, while free cross-border transfers of data are pursued, national measures to restrict or prohibit the cross-border transfers of data, known as data localization, are increasingly being adopted to retain "competitiveness" of nations.[18] The term "digital protectionism" seems to include this situation, although it is often used without definition.

Secondly, the presence of so-called non-trade issues is further increasing. Restrictions or prohibitions on cross-border data transfer are adopted for reasons other than the maintenance of "competitiveness." In particular, the protection of personal data or privacy has become one of the key issues in the rule-making on cross-border data transfers. For example, in the negotiations of WTO Joint Statement Initiative on E-Commerce (EC-JSI), there have been persistent difficulties in agreeing on the protection of personal information or personal data (see IV-2).[19]

New non-trade concerns have also emerged, cybersecurity being a key example.[20] The term cybersecurity is already widely used, but no universally agreed upon definition is said to exist.[21] However, there are several definitions, both internationally and domestically, and representatives are ones of the ISO/IEC and International Telecommunication Union (ITU) in the context of standardisation. According to the ISO/IEC, cybersecurity is defined as "safeguarding of people, society, organizations and nations from cyber risks (note 1 to entry: safeguarding means to keep cyber risk at a tolerable level)."[22] Domestic definitions include one by the US National Institute of Standards and Technology (NIST)[23] and the other by Japan's Basic Act on Cy-

---

[17] The Internet population reached 6% of the world's population in 2000 and 70% in 2022 (100% in Japan). ITU-D ICT Statistics. Facts and Figures <https://www.itu.int/itu-d/sites/statistics/>

[18] E.g., Digital Policy Alert, "Data Governance" <https://digitalpolicyalert.org/policy-area/data-governance?period=2020-01-01,2023-09-17>

[19] E.g., Inside US Trade (2023).

[20] E.g., Digital Policy Alert, "Data Governance" <https://digitalpolicyalert.org/policy-area/data-governance?period=2020-01-01,2023-09-17>

[21] Chang and Liu (2022) p. 186.

[22] ISO/IEC 27032:2023 (en) Cybersecurity — Guidelines for Internet Security < https://www.iso.org/standard/76070.html> For ITU, see ITU-T X.1205 (04/2008).< https://www.itu.int/rec/T-REC-X.1205-200804-I>

[23] NIST, Computer Security Resource Center, "Glossary" <https://csrc.nist.gov/glossary> One of the definitions of cybersecurity is "prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."

bersecurity (Act No. 104 of November 12, 2014).[24]

The term cybersecurity is often colored by politics and could be framed as a matter of internet sovereignty and national security.[25] The OECD has chosen to use "digital security," explaining that "'cybersecurity' has become a complex and multifaceted area" bringing together "at least four facets: economic and social; technical; law enforcement and national and international security." It describes that the economic and social facet of cybersecurity is digital security.[26] The OECD's careful approach reflects well that cybersecurity can have a political coloration. Such regulations from a cybersecurity perspective may restrict trade, ranging from measures that are essential for the smooth and secure digital trade, such as anti-phishing and online payment security, to measures introduced for national security reasons, and thus cybersecurity is an issue that is broadly relevant to digital trade as a whole.

Thirdly, the involvement of new "stakeholders" is emerging or increasing. The new "stakeholders" include governments and so-called digital platforms[27] as data holders, and consumers in general as producers of data (e.g. communication via SNS, online publication of their works, etc.) and as parties to online transactions. Some governments, as data holders, seek to localise data in order to maintain "competitiveness" or to use data as a means of surveillance and control of citizens, and in this sense, it is particularly compatible with autocratic regimes, which can be difficult to discipline internationally.[28] Some digital platforms aggressively collect data in order to provide their data-based services. In addition, in some cases, digital platforms are expected to play a certain regulatory role, including in terms of protecting personal data and preventing the

[24] Article 2 of the Basic Act on Cybersecurity defines cybersecurity in this Act as "the necessary measures have been taken to prevent the leakage, loss, or damage of information that is recorded, sent, transmitted, or received in electronic form, magnetic form, or any other form that cannot be perceived by the human senses (hereinafter referred to as "electronic or magnetic form" in this Article) and to securely manage that information in other such ways; that the necessary measures have been taken to ensure the security and reliability of information systems and of information and communications networks (including the necessary measures to prevent damage from unauthorized activities directed at a computer through an information and communications network or through a storage medium associated with a record that has been created in electronic or magnetic form (hereinafter referred to as "electronic or magnetic storage medium")); and that this status is being properly maintained and managed."

[25] Chang and Liu (2022) illustrate the Article 1 of the Cybersecurity Law (2917) of the PPR and the Law on Cybersecurity of Viet Nam (2018). In Article 2.1 of Viet nam's law, cybersecurity is defined as "the assurance that activities in cyberspace will not cause harm to infringe national security, social order and safety, or the lawful rights and interests of agencies, organizations and individuals." (English translation prepared by Allens Linklaters, https://www.allens.com.au/insights-news/insights/2018/06/vietnam-issues-a-stringent-new-cybersecurity-law/). Chang and Liu (2022), p. 187.

[26] The Global Forum on Digital Security for Prosperity (OECD). This forum is "an international multilateral and multidisciplinary setting for all stakeholder communities in this area." <https://www.oecd.org/digital/global- forum-digital-security/about/>

[27] Definitions of online platforms may vary, but one of the international definitions of an online platform is "a digital service that facilitates interactions between two or more distinct but interdependent sets of users (whether firms or individuals who interact through the service via the Internet)." OECD (2019), p. 21.

[28] Examples of how this is reflected in trade agreements are Articles 12.14 and 12.15 of the RCEP. (see V-2-1).

spread of fake news.[29] Consumers are increasingly directly involved in digital trade. Moreover, with the proliferation of AI, consumers are also affected by these technologies at a deeper level. For example, AI profiling can influence human decision-making and, in the case of generative AI, even intervene in human cognitive processes.[30] As these technologies may affect people at a deeper level than previous technologies, it seems important for consumers to be involved in the development of the relevant disciplines at an early stage. So far, trade agreements have sometimes used phrases such as "civil society" to provide for such engagement, albeit not necessarily in the context of digital trade.[31]

Fourthly, there is a growing digital divide and concern about it. The digital divide encompasses a variety of meanings, including differences in IT infrastructure between developed and developing countries, and internet penetration gender divide.[32] The former has been of particular concern to the international community. For example, WTO Members agreed at MC 12 to reinvigorate the work under the Work Programme on E-Commerce particularly in line with its development dimension.[33]

IV. Adaptation in Trade Agreements 1: WTO Agreements

To what extent have trade agreements adapted to digital trade and its challenges identified in the previous section? Current trade agreements can be broadly divided into WTO agreements and FTAs, and to summarise the overall picture, current WTO rules are limited in their response, while digital trade provisions are developing in FTAs to fill gaps in WTO rules, but their scope of application is limited to the parties to the agreement. Moreover, the content of these provisions in FTAs is "heterogeneous" in terms of the scope and depth of commitments.[34] In the following, both rules are examined in detail, starting with the WTO agreements and then the FTAs.

---

[29] An example is Articles 34 and 35 of the EU Digital Service Act (Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance), OJ L 277, 27.10.2022.). Both articles require providers of very large online platforms and of very large online search engines to diligently identify, analyse and assess any systemic risks in the Union stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services, and to put in place reasonable, proportionate and effective mitigation measures, tailored to the specific systemic risks identified thereof, with particular consideration to the impacts of such measures on fundamental rights.

[30] For example, if a state prepares and trains arbitrary answers in advance as answers to questions posed to the generative AI, humans may learn them from the generative AI.

[31] E.g., CPTPP Article 16.10 and USMCA Article 27.5 on participation of private sector and society, including civil society regarding the prevention of and the fight against corruption in matters affecting international trade or investment. JPN-EU Article 16.16 on joint dialogue with civil society in the Chapter 16 (Trade and Sustainable Development).

[32] WTO (2018) pp. 43-49.

[33] WT/MIN (22)/32(WT/L/1143) 22 June 2022. In addition, the 2023-2024 Aid-for-Trade Work Programme lists digital connectivity as one of priorities. WT/COMTD/AFT/W/95, 10 February 2023.

[34] E.g., Wu (2017) p. 8; Monteiro and Teh (2017) p. 71; Burri (2021) p. 20.

IV-1. WTO Agreements and Case Law

At present, digital trade encompasses at least digitally-enabled international trade in goods and services, including physically deliverable goods, and cross-border trade in data itself, which is underpinned by data, as discussed above. On this point, there is no agreement among WTO Members on the nature of digital goods—often referred to as "digital products," or e-commerce more broadly, as to whether they are goods or services. According to WTO jurisprudence, the service provided through electronic means can be classified at least in General Agreement on Trade in Services (GATS) mode 1 and a Member's commitment on a particular service sector in its GATS Schedule can cover the supply of such a service in non-physical form. In US - Gambling, the panel concluded that GATS mode 1 encompasses all possible means of supplying services through all means of delivery, whether by mail, telephone, Internet etc., unless otherwise specified in a Member's Schedule, noting that this is in line with the principle of "technological neutrality."[35] The panel appears to derive the principle from the Progress Report of the Work Programme on E-Commerce,[36] noting that it "seems to be largely shared among WTO Members."[37] This point was not appealed in this case.[38]

In addition, the Appellate Body (AB), in China - Publications and Audiovisual Products, considered whether China's commitment to "Sound recording distribution services" under the heading of "Audiovisual Services" extends to the distribution of sound recordings in non-physical form in the situation where foreign-invested enterprises were prohibited in electronic distribution of sound recordings, while like domestic service suppliers were not similarly prohibited in China.[39] The AB considered, in the process of interpretation, that "(m)ore generally… the terms used in China's GATS Schedule ("sound recording" and "distribution") are sufficiently generic that what they apply to may change over time," and concluded that its commitments cover both physical distribution as well as the electronic distribution of sound recordings.[40] The AB also considered "such reading of the terms in China's GATS Schedule to be consistent with the approach taken in US - Shrimp, where the AB interpreted the term 'exhaustive natural resources,'"[41] sug-

---

[35] Panel Report, United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services (US-Gambling) WT/DS285/R, para. 6.285.

[36] US-Gambling, footnote 836. Work Programme on Electronic Commerce – Progress Report to the General Council adopted by the Council for Trade in Services on 19 July 1999, S/L/74, 27 July 1999. para. 4: "It was also the general view that the GATS is technologically neutral in the sense that it does not contain any provisions that distinguish between the different technological means through which a service may be supplied."

[37] US-Gambling, para. 6.285.

[38] Appellate Body Report, United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services(US-Gambling(AB)), WT/DS285/AB/R, paras.219-220.

[39] Appellate Body Report, China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products (China-Publications and Audiovisual Products(AB)), WT/DS363/AB/R, paras. 338-339.

[40] China-Publications and Audiovisual Products (AB), para.398.

[41] China-Publications and Audiovisual Products (AB), footnote 705.

gesting so-called evolutionary interpretation.[42]

In addition to jurisprudence, some adaptations to digitalisation can also be found in the recently amended or concluded WTO agreements, such as Article 4.3 of the Agreement on Government Procurement—regulating procurement by electronic means—and the Article 17.2 (Electronic Payment) of the Agreement on Trade Facilitation. For the protection of personal data or privacy, there are relevant provisions in the general exceptions clause of the GATS[43] and in the Understanding on Commitments in Financial Services.[44]

In summary, the WTO has adapted to some extent to digital trade through concepts such as technological neutrality and evolutionary interpretation in dispute settlement procedures, and some agreements also address digital trade, albeit to a limited extent.

However, there are many gaps in the current WTO rules. To give some examples, the current classification of services (W/120) is outdated and the need for renegotiation has long been discussed.[45]

The classification of new services such as cloud services, SNS and online gaming is not necessarily clear,[46] nor is the classification of the delivery service Uber, the virtual meeting service Zoom or the chat service LINE.[47] In addition, there may be no WTO rules on the new challenges identified in the previous section. Only limited rules exist on cross-border transfers of data,[48] and no rules on data localisation or cybersecurity are found.[49] Moreover, "new stakeholders" do not seem to be envisaged enough. In short, the WTO Agreements, born in 1995, do not fully address digital trade, even though some developments have occurred.

Responding to such gaps through WTO dispute settlement procedures has its limits. As already mentioned, responding through the dispute settlement procedure involves relying on concepts such as technological neutrality and evolutionary interpretation. However, it is not always clear to what extent these concepts can take account of the development of digital trade and whether they are sufficiently clear in the context of digitalisation. For example, physical and non-physical delivery of sound recordings can be addressed, but what about the difference between AI-based and human-based service supply—can AI-based diagnostic imaging services

---

[42] For evolutionary interpretation, see Damme (2019) p. 171. The relevant part states that "(i)n practice, what is described as evolutionary interpretation is in essence often an effort to ensure that the treaty remains relevant and effective over time. In other words, evolutionary interpretation may often be understood as a choice, at the time of the interpretation of a treaty (and thus not necessarily at the time of its conclusion), to give meaning to a treaty taking into account developments subsequent to the conclusion of the treaty."

[43] GATS Article 14.c.ii.

[44] Understanding on Commitments in Financial Services para.8, "Transfers of Information and Processing of Information."

[45] Peng (2022) p. 6.

[46] Wu (2017) p. 5; Buri (2021) chapter.1.

[47] Peng (2022) pp. 6-7.

[48] Understanding on Commitments in Financial Services, para.8, "Transfers of Information and Processing of Information".

[49] The provision on the protection of personal privacy in the Understanding on Commitments in Financial Services and the security exceptions clauses such as GATT XXI, may cover part of the measures, but whether cybersecurity measures fall within the exceptions clauses is controversial. See V-2-2(3).

simply be seen as a different means of supply? Isn't the international community debating the regulation of AI, especially generative AI, because it is more than just an information service?[50]

There are also critical views on the principle of technological neutrality and evolutionary interpretation. On the former, in the panel proceedings in China - Publications and Audiovisual Products, China submitted that it has never been formally accepted by Members.[51] The panel noted while there is no need to invoke a principle of technological neutrality, it might have come into play had the panel found that China's commitment covered distribution on physical media and that there was doubt about whether it also covered the distribution of content on non-physical media,[52] finding that such a principle, whatever its status within the WTO, was likewise not needed in that case for the proper interpretation of China's commitment.[53] The panel appears to recognise the principle of technological neutrality on one hand, but also to suggest that its status is unclear on the other hand.[54] Indeed, the panel in US - Gambling referring to the principle of technological neutrality, only states that it is "largely shared," which does not mean that the principle is shared by Members as a whole. Moreover, the panel only states that it "seems to" be shared. The Panel also appeared to derive the principle of technological neutrality from the Progress Report of the Work Programme on E-commerce, but it could be argued that the panel may have placed too much reliance on such a report.[55] One commentator has raised the uncertainty of the status and role of the principle of technological neutrality in international trade law, including WTO agreements, and its potential of unpredictably expanding the scope of existing obligation and constraining the policy space of Members to adopt technology related regulations.[56]

The evolutionary interpretation is also controversial in relation to the development of technology. The evolutionary interpretation of China's Schedule of Commitments in China - Publications and Audiovisual Products was seen as a "positive development," but it was also stated that it does not necessarily help much to achieve legal certainty in such situations.[57] Particularly in the context of digital trade, "WTO case law is not entirely clear regarding in what situation and to what extent the `state of technology` that existed at the time of the negotiations is relevant in determining the

[50] On AI, international discussions have been ongoing, including on the need for development guidelines and a licensing system for the provision of services using advanced AI, in particular in the process known as the "Hiroshima AI Process" which was launched at the G7 Summit in May 2023. In December 2023, the Hiroshima AI Process Comprehensive Policy Framework was agreed and endorsed by the G7 leaders, along with the other relevant documents such as the Work Plan, which is the first international framework that includes guiding principles and the code of conducts to achieve the goal of safe, secure, and trustworthy AI. G7 Leaders' Statement December 6, 2023 <https://www.mofa.go.jp/files/100591757.pdf>

[51] China – Publications and Audiovisual Products, para.7.1249.

[52] China – Publications and Audiovisual Products, para.7.1258.

[53] China – Publications and Audiovisual Products, para.7.1264.

[54] As stated earlier, this issue was out of the AB proceedings. China –Publications and Audiovisual Products(AB), paras 219-220.

[55] The Panel appears to have found a normative effect in the Progress Report, and it is true that some "principles" have indeed been identified in the WTO dispute settlement procedures. Mitchell (2008), pp. 32-33, Part II.

[56] Gagliani (2020) pp. 731-738.

[57] Burri (2021) p. 19.

scope of the commitments."[58]

In any case, the limitation may be that some issues—such as the scope of Member's commitments in response to digitalization—that should essentially be decided by Members with "exclusive authority to adopt interpretation" and decision-making powers are instead addressed by these concepts.[59]

IV-2. Work and Negotiations in the WTO

In view of the limitations of the current rules, the WTO has addressed digital trade on two tracks: exploratory work and negotiations. The former is the multilateral track, created based on the Work Programme on Electronic Commerce adopted by Members in 1998, and the latter is the plurilateral track commenced following the Joint Statement on Electronic Commerce by a group of WTO Members in 2017.

The origin of the multilateral track dates back to the Declaration on Global Electronic Commerce in 1998, in which Members declared to "establish a comprehensive work programme to examine all trade-related issues relating to global e-commerce" and to "continue… current practice of not imposing customs duties on electronic transmissions" ("moratorium on e-commerce").[60] Subsequently, the Work Programme on E-Commerce was developed and discussions have continued on this basis since then, but as this was originally exploratory work rather than negotiation, it does not necessarily lead to rule-making. Nevertheless, the work deserves recognition in that it has involved all WTO Members and appears to have facilitated Members' understanding of digital trade.

The moratorium has generally been extended at each Ministerial Conference, but recently some developing countries have become increasingly reluctant for extension. Most currently it was agreed, at MC 13 in 2024, "to maintain the current practice of not imposing customs duties on electronic transmissions until the 14th Session of the Ministerial Conference or 31 March 2026, whichever is earlier...(and) (t)he moratorium and the Work Programme will expire on that date." In this Ministerial Decision, the wording of the extension did not include the part "unless Ministers or the General Council take a decision to extend," a change from the previous version.[61] In the future, the agreement on the extension is likely to be even tougher.

The plurilateral track was launched at the MC11 in 2017, when nearly 70 WTO members issued the Joint Statement on Electronic Commerce, in which they agreed "to initiate explor-

---

[58] Peng (2022) p. 778.

[59] Marrakesh Agreement Establishing the World Trade Organization, Articles XIV.2 and IV.1.

[60] WT/MIN(98)/DEC/2, 25 May 1998.

[61] WT/L/1193, 4 March 2024.

atory work towards future WTO negotiations on trade-related aspects of e-commerce."[62] This initiative on the Joint Statement on Electronic Commerce (EC-JSI) entered the negotiation phase in 2019.[63] The negotiations, led by co-convenors—Australia, Japan and Singapore—reached the substantial conclusion in December 2023 after five rounds of consolidated text releases based on participants' proposals.[64] Subsequently, in 2024, following the release and review of the Draft Chairs' Text and the announcement of finalizing "technical discussion,"[65] the participants announced the achievement of "stabilized text" on the Agreement on Electronic Commerce (EC).[66] Although these negotiations are on a plurilateral basis, nearly 90 countries participated on this announcement of the "stabilized text", and a successful conclusion would be significant in that it would provide new, almost multilateral rules for digital trade.

The Agreement on EC consists of 38 Articles and Annex. The Annex sets out principles on the regulatory framework for basic telecommunications services. The issues covered by the Agreement on EC include: electronic transactions framework; E-authentication and E-signatures; E-contracts; E-invoicing; paperless trading; single windows; electronic payments; customs duties on electronic transmissions; open government data; open Internet access; online consumer protection; unsolicited commercial electronic messages; personal data protection; cybersecurity; transparency; cooperation; development; telecommunications; exceptions. Articles on institutional arrangements and final provisions are also contained.[67] The discussions on the remaining issues, in particular, the legal question of how to incorporate the outcome into the WTO framework, seem to be continuing. Among the issues agreed upon, personal data protection has been particularly contentious between the EU, which takes a strict approach to the cross-border transfer of personal data to protect privacy, and the US, which, in contrast, takes a more lenient approach, so the agreement on this issue is very promising.

On the other hand, the articles on ICT products that use cryptography and data-related issues, namely, data flow—obligation to transfer data freely across borders, and data localisation—prohibition or restriction on requiring the establishment of computing facilities in the territory, and source code—prohibition or restriction on requiring the disclosure and transfer

---

62 WT/MIN(17)/60, 13 December 2017.

63 WT/L/1056, 25 January 2019.

64 WTO Joint Statement Initiative on E-commerce (WTO JSIE), "Co-Convenor Statement by Australia, Japan and Singapore 20 December 2023" <https://www.mofa.go.jp/mofaj/files/100598742.pdf >

65 WTO Press Release, 25 April 2024, "E-Commerce Negotiators Finalize 'Technical Discussions' and Outline Next Steps" <https://www.wto.org/english/news_e/news24_e/ecom_25apr24_e.htm>

66 INF/ECOM/87, 27 July 2024.

67 Ibid. Among these, e-payments, customs duties on e-commerce and development, together with cross-cutting issues such as preamble and exceptions had been outstanding issues at the stage of substantial conclusion. INF/ECOM/85/Rev.2. Although this is the restricted document, it has been reported by bilaterals.org and also referred to by Inside US Trade, "New WTO e-commerce text suggests negotiators closing in on deal", March 29, 2024.

of source code, which are of high interest to industry,[68] were not included in the "stabilized text."[69] One of the reasons for data-related issues not being included appears to be the change of position of the US—United States Trade Representative (USTR), which withdrew its support for the proposals on these issues in the EC-JSI negotiations in October 2023, a significant shift from its previous position.[70] Indeed, the US is not included in the announcement for the stabilised text,[71] being one of the remaining challenges of the EC-JSI.[72]

V. Adaptation in Trade Agreements 2: Pioneering FTAs

V-1. The Evolution of Digital Trade Provisions and the Rise of "Rule-Makers" in the FTAs

FTAs have served as "laboratories"[73] for regulating digital trade, filling the gaps in WTO agreements. The number of studies analysing these rules in FTAs is gradually increasing. One of the leading studies, Monteiro and Teh (2017)[74] pointed out at the time that, firstly, e-commerce provisions have been incorporated into an increasing number of FTAs; secondly, they are particularly heterogeneous in terms of structure, language and scope; and thirdly, they are likely to keep evolv ing.[75] Burri (2022) notes that out of the 370 FTAs, 203 FTAs contain digital trade provisions, based on TAPED database which reflects the digital trade provisions of the FTAs entered into force between 2000 and 2022.[76] According to Burri (2021), the number and level of detail of digital trade provisions in FTAs have increased significantly over the last 20 years or so, and in FTAs concluded between 2010 and 2019, digital trade provisions are included in nearly 70 percent of all FTAs on average, and data-related provisions can be also found, but only in a handful of agree-

---

[68] E.g., Inside US Trade (2024).

[69] The article on ICT was already decided not to be included in the Chairs' text. WTO Press Release, 25 April 2024 "E-commerce negotiators finalize "technical discussions" and outline next steps". Data-related issues were already identified as requiring "substantially more time for discussions" in December 2023, when the substantive conclusion was announced for 13 articles. WTO JSIE, "Co-Convenors Statement by Australia, Japan and Singapore 20 December 2023".

[70] USTR, "USTR Statement on WTO E-Commerce Negotiations", October 24 2023 < https://ustr.gov/about-us/policy-offices/press-office/press-releases/2023/october/ustr-statement-wto-e-commerce-negotiations> Support for non-discriminatory treatment of digital products also appears to have been dropped.

[71] INF/ECOM/87, 27 July 2024, note*.

[72] U.S. Mission Geneva, "Statement by Ambassador María L. Pagán on the WTO E-Commerce Joint Statement Initiative," July 26, 2024 <https://geneva.usmission.gov/2024/07/26/statement-by-ambassador-maria-l-pagan-on-the-wto-e-commerce-joint-statement-initiative/#:~:text=Geneva%2C%20Switzerland%2C-,July%2026%2C%202024,%2C%20governments%2C%20and%20the%20public>

[73] E.g., WTO (2018) p. 178.

[74] Monteiro and Teh (2017) cover the 275 RTAs in force at the time of analysis, notified to the WTO between 1957 and May 2017, that explicitly mention and refer to e-commerce.

[75] Monteiro and Teh (2017) p. 71.

[76] Burri (2022) p. 758. For TAPED Database, see TAPED: A Dataset on Digital Trade Provisions <https://www.unilu.ch/en/faculties/faculty-of-law/professorships/burri-mira/research/taped/>

ments, as a relatively new phenomenon.[77] Focusing on data-related provisions in FTAs based on the same Trade Agreement Provisions on Electronic-commerce and Data (TAPED) database, Elsig and Klotz (2021) identified 99 FTAs (82 countries involved, with the EU as one) that have at least one data-related provision, and considerable heterogeneity among FTAs.[78]

As can be seen, digital trade provisions have evolved over time and this trend has continued in the most recent period. Firstly, stand-alone digital trade agreements are emerging. The Japan-US Digital Trade Agreement, signed in 2019 and entered into force in 2020, was a pioneer in this respect, followed by the Digital Economy Partnership between Singapore, Chile and New Zealand (DEPA). In some cases, digital economy agreements are concluded to update the e-commerce chapter of existing FTAs, such as the Australia-Singapore Digital Economy Agreement (DEA)[79] and the UK-Singapore Digital Economy Agreement (UKSDEA).[80] The trade pillar of the IPEF, led by the US, is also negotiating digital trade rules.

Secondly, there have been developments in terms of number, detail, and scope in FTAs such as the EU's first inclusion of data-related provisions in FTAs, namely the EU-UK Trade Cooperation Agreement (EU-UKTCA).[81] Most of the stand-alone agreements or the recently concluded agreements to update the e-commerce chapters in the existing agreements have included provisions on new issues such as AI and digital identities (ID).

Thirdly, the "digital trade principles" are emerging, a more relaxed form than the agreement. A prime example is the EU, which has agreed on such principles, mainly as part of the "Digital Partnership," the core of which is cooperation on digital trade.[82] The most recent example is the EU-Singapore Digital Trade Principles (EUSDTP).[83] The G7 has also agreed such principles.[84]

There are key countries in the development of digital trade provisions described above. Burri (2021) and Elsig and Klotz (2021), using the same database but different approaches, identified common "central actors", "rule-makers" or "major drivers" of digital trade provisions, namely, the

---

[77] Burri (2021) pp. 20-26.

[78] Elsig and Klotz (2021) pp. 48-52.

[79] The DEA mainly updates the e-commerce chapter of the SAFTA, the FTA between the two countries.

[80] Digital Economy Agreement between the United Kingdom of Great Britain and Northern Ireland and the Republic of Singapore. UKSDEA mainly updates the e-commerce chapter of the FTA between the two countries.

[81] Trade and Cooperation Agreement between the United Kingdom of Great Britain and Northern Ireland, of the one part, and the European Union and the European Atomic Energy Community, of the other part.

[82] The EUSDTP, for example, consists of: 1) Preamble; 2) Digital Trade Facilitation; 3) Data Governance; 4) Consumer trust; 5) Business trust; and 6) Co-operation on digital trade.

[83] The EU-Singapore Digital Partnership / Digital Trade Principles (EUSDTP).

[84] The principles announced by the G7 in 2021 covers the following area: 1)open digital markets; 2) data free flow with trust; 3) safeguards for workers, consumers, and businesses; 4) digital trading systems, and 5)fair and inclusive global governance <https://www.meti.go.jp/press/2021/10/20211022008/20211022008-3.pdf>

US, Singapore, Australia, the recent EU, and Canada.[85]

The next section therefore looks at the more recent FTAs concluded by these countries and examines their response to the new challenges of digital trade. The reason for examining more recent FTAs is that, as mentioned above, the rules of FTAs have evolved over time. The agreements examined here are The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), The United-States-Mexico-Canada Agreement (USMCA), DEPA, DEA, UKSDEA, EU-UKTCA, EUSDTP and Regional Comprehensive Economic Partnership (RCEP), focusing on their e-commerce or digital trade chapters and other relevant chapters, including the financial services chapter, if the agreement is not a stand-alone agreement. RCEP is not an advanced FTA in this sense, but by including it, China, which is said to be one of the "WTO's three most powerful members" in terms of digital governance,[86] is also covered. Of the above, DEPA, DEA, UKSDEA and EUSDTP are stand-alone digital trade agreements, while DEA and UKSDEA replace existing digital trade provisions or chapters of FTA between the parties. It is worth noting that CPTPP and DEPA are open to new members and have the potential for expansion.[87] Before turning to how these agreements address the challenges, an overview of each agreement in the context of digital trade is provided below.

The CPTPP, signed and entered into force in 2018,[88] has an e-commerce chapter (chapter 14) consisting of 18 articles, and is said to have been partly rooted in SAFTA, an FTA between Australia and Singapore signed and entered into force in 2003.[89] Chapter 14 contains some of the most advanced provisions of its time and became the model for subsequent FTAs.[90] It includes new provisions not often found in previous trade agreements, such as provisions on data (Article 14.11 Cross-Border Transfer of Information by Electronic Means; Article 14.13 Location of Computing Facilities), source code (Article 14.17 Source Code) and cooperation on cybersecurity (Article 14.16 Cooperation on Cybersecurity Matters), which are subject to the dispute settlement chapter (Chapter 28), making them legally enforceable.

The USMCA, signed in 2018 and entered into force in 2020, has a chapter on Digital Trade

---

[85] Top countries that have entered into FTAs with e-commerce provisions are: (1) Singapore – 22 PTAs; (2) EU – 22 PTAs; (3) Australia – 15 PTAs; (4) United States – 14 PTAs; (5) Chile – 13 PTAs; (6) Canada – 12 PTAs; (number of FTAs). EU's FTAs have only recently included a specific chapter on e-commerce and some substantive provisions. Burri (2021) pp 20-21, ft. 53. The "central actors" or "rule-makers" in terms of data flow provisions are the EU, the US, Singapore, Australia, Canada and Mexico. Elsig and Klotz (2021) p. 53.

[86] E.g., Shaffer (2021) pp. 40-41.

[87] Under the DEPA, Korea's accession was substantially agreed in June 2023, and Canada, China, Costa Rica and Peru have already applied for accession. Joint Press Release <https://www.mti.gov.sg/Newsroom/Press-Releases/2023/06/Joint-Press-Release-on-the-accession-of-the-Republic-of-Korea> The potential for expansion of the DEPA is rather realistic, recalling how the US and other countries joined the negotiations for the P4 agreement, initially concluded by Singapore, Chile, New Zealand and Brunei, which led to the conclusion of the TPP in 2016 and ultimately to the CPTPP in 2018.

[88] The predecessor of this agreement, signed in 2016, was the Trans-Pacific Partnership Agreement.

[89] Examples include the non-discriminatory treatment of digital products in the CPTPP (Article. 14.4.1), and the protection of personal data (Article. 14.8). Wu (2017) pp. 10, 20.

[90] For example, the CPTPP was used as the basis for the USMCA negotiations. Peng (2022) ft.77. This is presumably because the US participated in the TPP negotiations and Mexico and Canada are parties to the CPTPP.

(Chapter 19) with 18 articles. It builds on the e-commerce chapter of the CPTPP, but develops its content with more robust data-related provisions, stronger protection of personal data, novel provisions on open government data (Article 19.18) and refined cybersecurity provisions (Article 19.15). These provisions are subject to the dispute settlement provisions of Chapter 31 and are therefore legally enforceable.

The DEPA, signed in 2020 and entered into force in 2021, is a stand-alone agreement on digital trade, consisting of 16 modules covering a wide range of digital trade-related issues.[91] Modules can be seen as chapters or sections of a trade agreement, with each module containing articles like a chapter or section of the trade agreement. The adoption of such a "modular" approach—"dividing the agreement into 'modules' covering rights and obligations under different digital economy issue areas"[92]—allows other countries to use the relevant modules when updating the existing FTAs and/or domestic policies, thereby extending its "normative impact" in addition to its possibility of new accession.[93] Nevertheless, most provisions originally focused on facilitating cooperation or best efforts obligations, and what was binding, if at all, was at best an obligation to cooperate. Legal enforceability was also limited, although it has a detailed dispute settlement procedure in Module 14.[94] However, the signing of the DEPA Protocol in July 2023 changed the situation and several controversial articles became binding and legally enforceable, such as Articles 3.3 (non-discriminatory treatment of digital products), 3.4 (ICT products using cryptography), 4.3 (cross-border information transfer by electronic means) and 4.4 (installation of computer equipment) . Still, controversial provisions such as financial services (Article 1.1.2.b, except Article 2.7 Electronic Payments), source code and algorithms are not covered. On the other hand, rather detailed obligations are stipulated for the protection of personal information[95] in Article 4.2 subject to Module 14.

The DEA, signed and entered into force in 2020, updates SAFTA's Chapter 14 (Electronic Commerce) into the new chapter 14 (Digital Economy) consisting of 38 articles and is one of the most comprehensive agreements on digital trade issues, including data-related provisions.

---

[91] The main provisions not included in the CPTPP and the USMCA are: Digital Identities (Article 7.1) in Module 7; Financial Technology Cooperation (Article 8.1), Artificial Intelligence (Article 8.2), Government Procurement (Article 8.3), and Cooperation on Competition Policy (Article 8.4) in Module 8 (Emerging Trends and Technologies); Data Innovation (Article 9.4) which considers trusted data sharing mechanism (Article 9.4); SME Cooperation in the digital sector (Module 10); and Digital Inclusion (Article 11.1), which specifies, among other things, the possibility of cooperation with civil society and others.

[92] Peng and Streinz (2021), p. 19.

[93] Ibid.

[94] DEPA Annex 14-A sets out the scope of application of Module 14, which excludes Articles 3.3 (non-discriminatory treatment of digital products), 3.4 (ICT products using cryptographic methods), 4.3 (cross-border information transfer by electronic means) and 4.4 (installation of computer equipment). According to Annex I (Understanding on this Agreement), these provisions do not create any rights or obligations between or among the parties. However, the Protocol to DEPA, signed in July 2023, ceases the operation of Annex 14-A and Annex I so that these provisions become legally binding and subject to dispute settlement procedures upon entry into force. The Protocol enters into force 60 days after the last party notifies the DEPA Depositary of the completion of its applicable legal procedures.

[95] The definition of personal information (Article 1.3) is identical to that in the CPTPP.

This is reflected in the title of the chapter being "digital economy" rather than e-commerce or digital trade. Moreover, it not only appears to be inspired by the DEPA, such as provisions on digital ID (Article 29), AI (Article 31) and Fintech (Article 32), but also covers novel issues that go beyond the DEPA: the inclusion of financial services in provisions on location of computing facilities (Article 25); submarine telecommunications cable systems from the perspective of ensuring infrastructure stability (Article 22); and cooperation on RegTech in addition to FinTech (Article 32). It also covers broader issues related to the digital economy, such as cooperation on competition policy (Article 16) and stakeholder engagement (Article 35), and shows a strong recognition of bridging the digital divide, reflected in the provisions on SMEs (Article 36) and capacity building (Article 37). A number of provisions are subject to Chapter 16 (Dispute Settlement), and are therefore legally enforceable.

The UKSDEA, signed and entered into force in 2022, also covers a wide range of issues in Section F of Chapter 8, entitled "Digital Trade and the Digital Economy", and even goes further than the DEA, which similarly applies to the "digital economy." It applies to the novel issues, such as "Lawtech," and enhances the provisions on cybersecurity based on the relevant provisions of the USMCA (see V-2-2(3)). There are also a number of mandatory provisions, which are covered by the dispute settlement chapter (Chapter 14) .

The EU-UKTCA, signed in 2020 and entered into force in 2021, is the first EU trade agreement to include a chapter on digital trade, which is subject to dispute settlement procedures. Its volume is extensive, but the key provisions on digital trade can be found in Part Two (Trade, Transport, Fisheries and Other Arrangements) Heading One (Trade) and Title III (Digital Trade).[96] Compared to the other agreements, the number of provisions and the coverage are rather limited, and its distinctive features are: unique structure for data-related provisions; "right to regulate" provision (see V-2-2(2)); emphasis on the protection of personal data and privacy (see V-2-2(2)); enhanced relationship with trade in services[97]; and cooperation on regulatory issues.[98]

The EUSDTP, the principles signed in 2023, looks like a basis for an agreement, because it contains sophisticated provisions that could be applied simply by changing the relevant

[96] Title III consists of three chapters: Chapter 1 General Provisions (Articles 196-200); Chapter 2 Data Flows and Personal Data Protection (Articles 201, 202); and Chapter 3 Specific Provisions (Articles 203-212) (17 articles in total). In addition, cybersecurity is addressed separately as part of thematic cooperation (Part Four (Thematic Cooperation) Title II (Cyber Security)), dispute settlement separately (Part Six (Dispute Settlement and Horizontal Provisions) Title I (Dispute settlement)) and personal data protection-related provisions in several chapters.

[97] Examples include the provision confirming electronic transmission being considered as the supply of a services in the relevant chapter (Art.203.1), and the provision in Title III (Digital Trade) providing for the understanding of the parties on computer services, which extends the scope of "computer services."

[98] EU-UKTCA Article 211 Cooperation on Regulatory Issues with regard to Digital Trade.

wording to "shall," although they are not legally binding at this stage.[99] Indeed, in July 2023, the parties to the agreement announced that they would start negotiations on a digital trade agreement "building on the cooperation and convergence" in EUSDTP and the EU-Singapore Digital Partnership, the basis of the Principles.[100] The EUSDTP is novel in that it covers issues not addressed by the EU-UKTCA, such as AI and detailed provisions on technical regulations and conformity assessment.

The RCEP, signed in 2020 and entered into force in 2022, has a chapter on e-commerce (Chapter 12) with 17 basic articles covering the issues agreed in EC-JSI negotiations and in GATS including a provision for online personal information protection (Article 12.8), as well as data-related provisions (Article 12.14 Location of Computing Facilities; Article 12.15 Cross-border Transfer of Information by Electronic Means). However, the overall level of the rules is not so ambitious, as it provides for broad exceptions to data-related provisions (see V-2-2),[101] and the dispute settlement procedures in Chapter 19 do not currently apply to Chapter 12. On the other hand, an innovative feature is that the Dialogue on E-Commerce (Article 12.16; Article 18.3.1.j) may include participation from the business sector, experts, academia, and other stakeholders as appropriate, thus providing an opportunity for stakeholder involvement.

In light of the above, the next section presents cross-agreement examinations from the following perspectives: 1) new trade-restrictive measures (data-related provisions); 2) digital trade-related non-trade concerns; 3) new "stakeholder" involvement; 4) digital divide; and 5) other issues. In the examination, in addition to the substantive rights and obligations, the preamble of the agreements and the recognition of the parties expressed in the provisions are considered. These do not set out the rights and obligations of the parties, but are said to have a certain significance. The preamble can have an important contribution to treaty interpretation,[102] as it forms part of the context within which a treaty should be interpreted and it also clarifies its object and purpose.[103] As for the provisions setting out the "recognition" of the parties, it was noted that they are valuable in that they provide a basis for the general expec-

---

[99] Singapore and the European Union Sign Digital Partnership, 1 February 2023 para.20. <https://digital-strategy.ec.europa.eu/en/library/eu-singapore-digital-partnership>; EUSDTP Preamble 9th recital. Hereinafter, the numbering of the articles is based on the Principles published by the EU. EU, "Digital Trade Principles" <https://policy.trade.ec.europa.eu/help-exporters-and-importers/accessing-markets/goods-and-services/digital-trade_en>

[100] "Joint Statement on the Launch of Negotiations for an EU-Singapore Digital Trade Agreement" <https:// policy.trade.ec.europa.eu/news/joint-statement-launch-negotiations-eu-singapore-digital-trade- agreement-2023-07-20_en> On 25 July 2024, they announced the conclusion of the negotiation <https://ec.europa.eu/commission/presscorner/detail/en/IP_24_3982>

[101] The treatment of digital products, source code, cross-border data flow, and the location of computing facilities in financial services, among others, remain to be the matters for future dialogue. (Articles 12.16.1 (b) and (c)). These issues will be subject to a general review of the RCEP, which will be undertaken five years after the date of entry into force, and every five years thereafter, unless the parties agree otherwise (Article 20.8), and the parties are obliged to consider them (Article 12.16.1).

[102] Vienna Convention on the Law of Treaties, Article 31.2.

[103] E.g., Gleason and Titi (2022) p. 7.

tations of the parties and may also define the future direction of the subject matter,[104] while providing a clue to the discussions that took place during the negotiations.[105] Again, although not immediately legally binding, both can hopefully gradually affect the policies of parties.[106]

V-2. Cross-Agreement Examinations

V-2-1. Response to New Trade-Restrictive Measures: Data-Related Provisions

The data-related provisions regulating cross-border data transfers and data localization measures are included in all the agreements examined in this paper. The essence of these provisions is generally to allow the cross-border transfer of data or information by electronic means, and to prohibit the requirement to use or install computer facilities in the party's territory as a condition for conducting business in that territory. The origin of these provisions is CPTPP (Articles 14.11[107] and 14.13[108]), but the relevant provisions of the CPTPP do not cover financial services. For financial services, provisions on cross-border data transfers were found in agreements other than DEPA and EUSDTP, while provisions on location of computing facilities, regulating localization, were found in agreements except CPTPP, DEPA, EUSDTP and RCEP (Table 1 in the Appendix. Highlights for the remainder of this section are also provided in Table 1).

In addition, these data-related provisions are accompanied by legitimate public policy objective (LPPO) "exceptions," which provide that the parties shall not be prevented from adopting or maintaining measures to achieve a LPPO under certain conditions (but see below

---

[104] In the context of cyber security, Whitsitt (2023) p. 18.

[105] Kimura (2022) p.1570.

[106] Peng (2022) p. 786.

[107] CPTPP 14.11 Cross-Border Transfer of Information by Electronic Means

1. The Parties recognize that each Party may have its own regulatory requirements concerning the transfer of information by electronic means.
2. Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person.
3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:
   (a) 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 transfers of information greater than are required to achieve the objective.

[108] CPTPP Article 14.13: Location of Computing Facilities

1. The Parties recognize that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications.
2. No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.
3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:
   (a) 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.

for USMCA and EU-UKTCA). Certain conditions include that the measure: (a) 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 transfers of information greater than are required to achieve the objective. Financial services may be subject to other conditions or requirements. In terms of enforcement, the data-related provisions are covered by the respective dispute settlement procedures, with the DEPA and RCEP.

It is worth noting that the USMCA contains notably strong language on data-related provisions. Article 19.11 (Cross-Border Transfer of Information by Electronic Means)[109] of the USMCA, like the CPTPP, allows for the LPPO "exceptions", but by inserting "necessary" in the article to achieve the LPPO, it seems to raise the threshold for parties to take such LPPO measures. The provisions on the location of computing facilities don't provide for the LPPO "exceptions" as found in other agreements in the first place (Article 19.12 Location of Computing Facilities).[110]

The EU-UKTCA has a unique structure for data-related provisions. Under Article 201 (Cross-Border Data Flows), the parties are committed to ensure cross-border data flows, and such flows shall not be restricted between the parties by a party: (a) requiring the use of computing facilities or network elements in its territory for processing; (b) requiring the localization of data in its territory for storage or processing; (c) prohibiting the storage or processing in the territory of the other Party; or (d) making the cross-border transfer of data contingent upon use of computing facilities or network elements or upon localisation requirements, both in its territory.[111] The LPPO "exceptions" appears to be treated as a "right" (Article 198 Right to Regulate) that distinguishes it from other agreements, accompanied by the illustrative list of "legitimate policy objectives" (LPOs). This structure seems to provide rather powerful exceptions rather than the LPPO "exceptions," but raises other issues, which are discussed in the next section (see V-2-2(1)).

The RCEP provides for broader LPPO "exceptions" and security exceptions to data-related provisions than other agreements. The RCEP prohibits a party to require a covered per-

---

[109] USMCA Article 19.11 Cross-Border Transfer of Information by Electronic Means

1. No Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person.
2. This Article does not prevent a Party from adopting or maintaining a measure inconsistent with paragraph 1 that is necessary to achieve a legitimate public policy objective, provided that the measure:
   (a) 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 transfers of information greater than are necessary to achieve the objective.(*Footnote 5 omitted*)

[110] USMCA Article 19.12 Location of Computing Facilities

No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.

[111] The parties shall keep the implementation of this provision under review and assess its functioning within three years of the date of its entry into force. A party may also propose to the other party to review (a)-(d), and the other party shall accord a sympathetic consideration (Article 201.2).

son[112] to use or locate computing facilities in its territory as a condition for conducting business in its territory (Article 12.14.2), and to prevent cross-border transfer of information by electronic means where such activity is for the conduct of the business of a covered person (Article 12.15.2). However, it explicitly states that any measure inconsistent with these prohibitions that it "considers necessary" is permissible, provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade (Articles 12.14.3.a, 12.15.3.a), and that the determination of the necessity is made by the party implementing the measure (footnotes to both Articles). Currently, the e-commerce chapter is not covered by Chapter 19 (Dispute Settlement),[113] but even if these articles were to be covered by Chapter 19, the broad scope of the LPPO "exceptions" and the self-judging nature of necessity will leave only the fulfilment of the conditions of the applications of the measure to be challenged by other parties. In addition, the security exceptions clause provides also that a party shall not be prevented from adopting or maintaining any measure it considers necessary for the protection of its security interests and that such a measure shall not be disputed by other parties (Articles 12.14.3.b, 12.15.3.b). These give extensive discretion to the party taking a measure with almost no room for challenge by other parties. Such RCEP provisions could lead to legal instability, which in turn could render the prohibitions themselves meaningless.

Overall, the agreements examined in this paper contain provisions on new types of trade-restrictive measures, but further refinement of the provisions is possible to address issues such as localisation measures for financial services.

V-2-2. Response to Digital Trade-Related Non-Trade Concerns

(1) "Right to Regulate" and LPPO

In terms of non-trade concerns, the first thing to point out is the growing recognition of the "right to regulate" by the parties. In the agreements examined in this paper, references to the "right to regulate" are mainly found in the preambles of the agreements. In some cases, the preamble also refers to "legitimate public welfare objectives" (LPWOs) together with the "right to regulate" and illustrates its content: the CPTPP; the USMCA; the DEA; and the UKSDEA. The DEPA, the EUSDTP and the RCEP don't provide illustrations. The preamble of the CPTPP, for example, refers to the Parties' inherent right to regulate and their resolve

[112] A covered person means, a covered investment, an investor of a party or a service supplier of a party, but does not include a financial institution, a public entity, or a financial service supplier, each as defined in the relevant chapter (Article 12.1. b).

[113] At present, chapter 19 (Dispute Settlement) is not applicable to chapter 12 on e-commerce. The only recourse is consultations and referral of the matter to the RCEP Joint Committee if difference arises between the parties on the interpretation and application of the chapter 12 (Article 12.17.1 and 2). The parties shall review the application of chapter 19 to chapter 12 as part of the general review under Article 20.8, which will be undertaken five years after its entry into force and every five years thereafter, unless the parties agree otherwise. However, even if such application is agreed in the review, it shall be limited to the parties that have agreed to its application (Article 12.17.3).

to protect LPWOs, such as public health, safety, the environment, the conservation of living or non-living exhaustible natural resources, the integrity and stability of the financial system, and public morals. The DEA updating the SAFTA's e-commerce chapter makes a new reference to the "right to regulate" in the preamble, while the SAFTA preamble makes no mention of such rights, suggesting that the introduction of digital trade rules was the motivation for such a reference.[114] This willingness of the parties is reflected in the fact that the LPPO "exceptions" is provided for in the data-related provisions. Among others, the EU's commitment to regulatory autonomy is striking: EU-UKTCA Title III "Digital Trade" provides for the "right to regulate" itself in Article 198, with an illustration of the LPOs,[115] and it also confirms that nothing in Title III prevents the parties from adopting or maintaining measures in accordance with Articles 184 (Prudential Carve-Out), 412 (General Exceptions) and 415 (Security Exceptions) for the public interest reasons set out therein.[116]

However, the concepts of "right to regulate" and LPPO are not so clear. There are LPPO "exceptions" in data-related provisions, the "right to regulate" enshrined in the preamble with the concept of LPWO, and a similar concept, LPOs, with its illustrative list set out in the EU-UKTCA.[117] The content of the illustrations is similar, but there are also some nuanced differences. While they are all illustrative, and what constitutes legitimate policy objectives may, of course, vary according to the circumstances of each country, including level of development, economic situation, and social and cultural differences, the concern is the possibility that the scope of "exceptions" may be broadened, rendering the rules meaningless.

The "right to regulate" in EU-UKTCA can also raise another issue, namely the relationship with the exceptions clauses.[118] Article 198 (Right to Regulate) provides that the parties reaffirm the right to regulate within their territories to achieve LPOs such as the protection of public health, social services, public education, safety, the environment including climate

---

[114] DEA Annex B Preamble (relevant part only and emphasis added)
"Recognising their inherent right to regulate and resolving to preserve their flexibility to set legislative and regulatory priorities, safeguard public welfare and protect legitimate public welfare objectives, such as public health,safety, the environment, privacy, the conservation of living or non- 37 living exhaustible natural resources, the integrity and stability of the financial system and public morals;"

[115] EU-UKTCA Article 198 Right to regulate
The Parties reaffirm the right to regulate within their territories to achieve legitimate policy objectives, such as the protection of public health, social services, public education, safety, the environment including climate change, public morals, social or consumer protection, privacy and data protection, or the promotion and protection of cultural diversity.

[116] EU-UKTCA Article 199 Exceptions
For greater certainty, nothing in this Title prevents the Parties from adopting or maintaining measures in accordance with Articles 184, 412 and 415 for the public interest reasons set out therein.

[117] Moreover, the preamble of EU-UKTCA refers to the parties' respective rights to regulate to achieve LPPO and the illustration thereof. (Preamble, "7. RECOGNISING the Parties' respective autonomy and rights to regulate within their territories in order to achieve legitimate public policy objectives such as...")

[118] With the exception of EU-UKTCA, GATT Article XX and GATS Article XIV, or only GATS Article XIV, are applied, mutatis mutandis, either in whole or in part, for the general exceptions. In EU-UKTCA, GATT Article XX is applied mutatis mutandis, but with additional elements such as further conditions. GATS Article XIV is not referred to, but some similar rules are provided (Article 412). (With the exception of EUSDTP, which does not provide for exceptions clauses as being principles).

change, public morals, social or consumer protection, privacy and data protection, or the promotion and protection of cultural diversity. In parallel, Article 199 (Exceptions) provides that, as noted above, nothing in Title III prevents the parties from adopting or maintaining measures in accordance with the exceptions clauses (Articles 184, 412 and 415) in other chapters for the public interest reasons therein. As there is some overlap between LPOs and "public interest reasons," the relationship between the two is somewhat ambiguous and raises the following questions. Suppose a party takes a measure to restrict cross-border flows of certain data to protect cultural diversity. What would be the legal nature of the measure whereas such a cause is not included in the exhaustive list of Article 412 (General Exceptions)? Does such a measure naturally fall within the scope of a right to regulate provided for in Article 198, and if so, are such measures unlimited, since the list contained therein is only illustrative? In particular, one of the differences between Article 198 and Article 412, which incorporates General Agreement on Tariffs and Trade (GATT) Article XX mutatis mutandis, is that there is no chapeau setting out the requirements for the application of the measure, which could lead to possible abuse. Or is the right to regulate under EU-UKTCA is subject to certain limitations? Furthermore, to what extent do "LPPO" and "LPO"—the difference being "public"—differ from each other? These points deserve further consideration.

(2) Personal Information Protection

The protection of privacy, which was one of the grounds for exceptions in the GATS, is now an obligation on the parties, in the agreements considered in this paper, to adopt or maintain a legal framework that protects the personal information of "users of digital trade" (e.g., USMCA Article 19.8) or "persons who conduct or engage in electronic transactions" (e.g., DEA Article 17), with the exception of the EUSDTP, as being principles not providing binding obligations. The EU-UKTCA provides a right rather than an obligation, as discussed later.

In particular, the DEPA contains very detailed provisions and refers to specific ways in which personal information can be transferred across borders. DEPA Article 4.2 (Personal Information Protection) prescribes the parties' recognition on the importance of protecting the personal information of participants in the digital economy (para.1), and obliges each party to adopt or maintain a legal framework that provides for the protection of the personal information of the users of e-commerce and digital trade (1st sentence of para.2).[119] In developing such a framework, it obligates each party to take into account principles and guidelines of relevant international bodies (2nd sentence para.2), and exemplifies eight principles as underpinning the legal framework (para.3). These correspond to the so-called OECD Principles on

[119] E-commerce and digital trade are distinguished, but neither is defined.

privacy.[120] It also mandates each party to adopt non-discriminatory practices in protecting users of e-commerce from personal information protection violations occurring within its jurisdiction (para.4), to publish information on such protections it provides to such users (para.5), and to purse the development of mechanism[121] and exchange information, including on the application of that mechanism, in order to promote compatibility and interoperability between the parties' different regimes (paras.6 and 7). It extends the parties' obligations to data protection trustmarks to encourage business for adoption of such marks, to exchange information and share experiences on their use, and to endeavour mutual recognition of each trustmark as a valid mechanism for facilitating cross-border information transfer while protecting personal information (paras. 8,9 and 10). This article is subject to DEPA Module 14 (Dispute Settlement) and entails legal enforceability. By including personal information protection in trade agreements, the DEPA case seems to reinforce the recent trend of FTAs having tendencies to extend their scope to include non-trade issues such as environment and labour, in some cases even the link with trade being diluted.[122]

In terms of personal information protection, the EU is known for its high standards of protection of personal data as a fundamental right.[123] The EU-UKTCA confirms the EU's strong commitment to the protection of personal data and privacy.[124] In Title III, Chapter 2 entitled "Data Flows and Personal Data Protection," the protection of personal data and privacy is explicitly stated as a "right" of individuals[125] and another chapter of the agreement confirms this stance (Article 769 Personal Data Protection). The EU's high standards in this regard also differ from the relatively lax stance of the US and others, and have been one of the challenges in developing international rules for digital trade.

However, the trade agreements examined in this paper show some promising developments in this matter in that the EU is addressing it in its trade agreements. Previously, the EU

---

[120] OECD Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, which includes eight principles: 1) Collection Limitation Principle; 2) Data Quality Principle; 3) Purpose Specification Principle; 4) Use Limitation Principle; 5) Security Safeguards Principle; 6) Openness Principle; 7) Individual Participation Principle; and 8) Accountability Principle.

[121] The mechanisms illustrated are: the recognition of regulatory outcomes or mutual arrangement; broader international frameworks; national trustmark or certification frameworks; or other avenues of transfer of personal information between the parties.

[122] For example, the CPTPP and the USMCA provide that no party shall fail to effectively enforce its environmental laws "in a manner affecting trade or investment between the Parties," but the USMCA is more lax on the standard of proof, as failure is presumed to be in such a manner unless the responding party proves otherwise in the dispute settlement process (CPTPP Article 20.3.4, USMCA Article 24.4.1).

[123] TFEU Art.16.1, Charter of Fundamental Rights of the EU Article 8.1. See also, Ishii (2017) pp.3-4.

[124] Personal data is defined as "any information relating to a data subject" (Article 6.1.d).

[125] EU-UKTCA Article 202 Protection of Personal Data and Privacy

1. Each Party recognises that individuals have a right to the protection of personal data and privacy and that high standards in this regard contribute to trust in the digital economy and to the development of trade.
2. Nothing in this Agreement shall prevent a Party from adopting or maintaining measures on the protection of personal data and privacy, including with respect to cross-border data transfers, provided that the law of the Party provides for instruments enabling transfers under conditions of general application1 for the protection of the data transferred.
3. Each Party shall inform the other Party about any measure referred to in paragraph 2 that it adopts or maintains.

could not make the protection of personal data the subject of trade negotiations, reportedly due to a disagreement between the trade and justice departments of the European Commission over how to deal with cross-border transfers of data in trade agreements while ensuring the protection of personal data.[126] However, in 2018, the EU approved a "Horizontal Provisions on Cross-border Data Flows and Personal Data Protection" (Horizontal Provisions).[127] Some bilateral negotiations based on Horizontal Provision have been successful and, reportedly, have been proposed in the context of the EC-JSI negotiations.[128] The EU-UKTCA also reflects some of the Horizontal Provisions. On this point, the European Data Protection Supervisor (EDPS) has strongly criticized the EU-UKTCA for not reflecting all of the Horizontal Provisions[129] and some view that EU Member States are still divided on the use of them.[130] Nevertheless, the fact that the EU is addressing the protection of personal data and privacy in its trade agreements is in itself a hopeful sign of progress on this issue.[131]

The US attitude also appears to be changing. CPTPP Article 14.8 (Personal Information Protection), largely following the TPP, which reflects the US position, imposes an obligation to adopt or maintain a legal framework providing for the protection of personal information of e-commerce users, but is relatively more lax in its content: parties "should" rather than "shall" take into account the principles and guidelines of relevant international bodies; and no reference is made to the OECD Principles (2013)[132] or the Asia Pacific Economic Cooperation (APEC) Privacy Framework,[133] while some other agreements examined in this paper explicitly mention them. This is partly due to the fact that privacy in the US is said to focus on protecting citizens from the collection and use of information by government rather than by private actors, combined with the absence of an official data protection authority, with self-regulation and best practices being the common model of privacy protection.[134] Howev-

---

[126] Aaronson and Leblond (2018) pp. 261-262. As a result, Japan-EU EPA, for example, only included the review clause, which stipulates that the provisions on the free flow of data shall be reassessed within three years of the date of its entry into force (Article 8.81). They then agreed to negotiate this provision in October 2022, reached substantive agreement a year later, and signed the agreement in January 2024. EU, Press Release <https://www.consilium.europa.eu/en/press/press-releases/2024/01/31/eu-japan-economic-partnership-agreement-eu-and-japan-sign-protocol-to-include-cross-border-data-flows/>

[127] "Horizontal Provisions on Cross-border Data Flows and Personal Data Protection" <https://ec.europa.eu/newsroom/just/items/627665/en>

[128] E.g. "Recommendation for a Council Decision authorising the opening of negotiations for the inclusion of provisions on cross-border data flows in the Agreement between the European Union and Japan for an Economic Partnership, Brussels, 12.7.2022 COM (2022) 336 final", <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0336>

[129] "opinion/ 22 Feb 2021" <https://edps.europa.eu/press-publications/press-news/press-releases/2021/data-protection-non-negotiable-international_en>

[130] Zhang (2021) pp. 7-8.

[131] The Horizontal Provisions are reflected also in EU-NZ FTA, signed in 2023 and entered into force in 2024.

[132] OECD Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013).

[133] APEC Privacy Framework was introduced in 2004 and revised in 2015. <https://www.apec.org/groups/committee-on-trade-and-investment/digital-economy-steering-group>

[134] Burri (2021) p. 753.

er, in USMCA, parties' obligations to protect personal information[135] have been strengthened (Article 19.8): reference to the OECD Principles and the APEC Framework as those that should be taken into account (para.2); illustration of 9 key principles,[136] including those in the OECD Principles; recognition of the importance of ensuring compliance with measures to protect personal information and their proportionality to the risks; and an obligation for each party to publish information on the personal information protection it provides to users of digital trade, including the means for a natural person to pursue a remedy. The USMCA even sets out personal information protection more generally, not limited to digital trade, which has similar provisions (Article 32.8).[137] Such a changing US response is further confirmed by trends in the US, where relevant federal bills are being introduced in Congress.[138]

Of the trade agreements examined in this paper, there is a degree of convergence on personal information protection, with the exception of the EU-UKTCA. The post-CPTPP agreements provide for the consideration of principles and guidelines when developing the legal framework for the protection of the personal information, and in some cases, there are references to the OECD Principles and the APEC Framework (e.g., DEPA Article 4.2; DEA Article 17.3; UKSDEA Article 8.61E). Even without specific reference to them, the content of the eight OECD principles may be included (e.g. Articles 4.2 of DEPA, 17.3 of DEA, 8.61E of UKSDEA), and/or the APEC CBPR[139] may be strongly promoted (e.g. USMCA Article 19.8.6; DEA Articles 17.8 and 17.9). Given the different approaches between countries, as in the case of the EU and the US, the possibility of adopting different approaches and ensuring their interoperability, and the specific methods for doing so, are sometimes provided for on personal information protection (e.g. DEPA Article 4.2.6; DEA Article 17.7; UKSDEA Article 8.61E.6).

An interesting development in recent years in terms of ensuring interoperability is the operation of the Global CBPR, a certification mechanism for cross-border data transfer while ensuring the protection of personal information.[140] Under this mechanism, companies are certified if they meet the requirements for cross-border data transfers. While the APEC CBPR was originally developed to certify compliance with the APEC Privacy Framework, the participating economies—9 countries and regions, including Japan—announced the launch of

[135] USMCA Article 19.1 defines personal information as "information, including data, about an identified or identifiable natural person," almost identical to the CPTPP.

[136] In USMCA, "transparency" replaces 6) Openness among the eight OECD principles, and "choice" is added.

[137] The definition of personal information in this article is "information, including data, about an identified or identifiable natural person," which is the same as the definition in Chapter 19.

[138] E.g., H.R. 8152 submitted to the 117th Congress. <https://www.congress.gov/bill/117th-congress/house-bill/8152/text>

[139] APEC Cross-Border Privacy Rules. <https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System>

[140] These transfer mechanisms mainly include: accountability principle; assessment of the level of data protection in destination countries ("adequacy"); contracts; binding corporate rules; certifications; and consent. OECD (2023) pp. 23-30.

the Global CBPR in April 2022 to facilitate the smooth cross-border transfer of personal information in a wider area than APEC, and to promote interoperability between national legal frameworks.[141] In April 2023, the organisational documents of the Global CBPR, including the Global CBPR Framework and the Forum's Terms of Reference, were released, making new participation by interested jurisdictions possible.[142] The UK was the first to apply and was granted Associate status under less stringent participation requirements.[143] However, the relationship between the global CBPR and the existing APEC CBPR, as well as the EU certification system, which has been coordinated for many years, needs to be clarified in order to increase the legal certainty for businesses.[144] In particular, the challenge will be to ensure mutual recognition of certification between the two.

It remains to be seen whether these developments will lead to a further convergence of provisions on the protection of personal information in trade agreements.

(3) Cybersecurity

All of the agreements reviewed in this paper contain some kind of provision on cybersecurity, suggesting that it is a common interest for all, especially those that are leading the way in disciplining digital trade.[145] With the exception of the EU-UKTCA,[146] the agreements covered can be broadly categorized, according to the level of sophistication of the provisions, into those that only prescribe the parties' recognition on the importance of cybersecurity (CPTPP, DEPA, DEA, RCEP), and others, including USMCA (Article 19.15 Cybersecuri-

[141] Global CBPR Forum, "About the Global CBPR Forum". <https://www.globalcbpr.org/about/>

[142] Global CBPR Forum, News, April 13, 2023 "Global CBPR Forum Welcomes Participation by Interested Jurisdictions". <https://www.globalcbpr.org/global-cross-border-privacy-rules-cbpr-forum-welcomes-participation-by-interested-jurisdictions/>

[143] Global CBPR Forum, News, July 6, 2023 "The Forum Welcomes the UK as an Associate". <https://www.globalcbpr.org/the-forum-welcomes-the-uk-as-an-associate/>

[144] According to the OECD (2023), which surveyed cross-border data transfers and the experiences of business, the increase in data protection and privacy laws in various countries, while contributing to the protection of privacy, can also increase regulatory risks for companies due to the overlapping obligations to comply with various regulations. The main challenges for business are the legal uncertainties, which should be addressed through increased transparency of in privacy related laws on the data transfer requirements (e.g., ambiguities in the definition of "data transfer to a third country" and the lack of a clear distinction in the law between data controllers and data processors"), cross-sectoral consistency of regulations (e.g. financial and other data, and critical national infrastructure-related data and other data). OECD (2023) pp. 11-18.

[145] Cybersecurity provisions in trade agreements fall under provisions with titles such as "cybersecurity" or "cooperation on cybersecurity" in a narrow sense, but more broadly could include provisions such as DEA Article 18 Creating a Safe Online Environment and DEA Article 5.2 Online Safety and Security, as well as provisions relating to the access to source code (or algorithms in source code) for cybersecurity reasons (e.g. USMCA Article 19.16). This paper considers the cybersecurity provisions in the narrow sense, as well as the security exceptions clauses discussed below.

[146] In the EU-UKTCA, cybersecurity is stipulated as one of the areas of cooperation.

ty),[147] that stipulate additional elements such as cooperation, and those that extend USMCA (USMCA, UKSDEA, EUSDTP), referred to as "USMCA model" in this section.

The basic elements of the USMCA model, in addition to the above-mentioned recognition, are mainly: 1) building the capabilities of the parties' respective national entities responsible for responding to cybersecurity incidents; 2) cooperation between the parties to identify and mitigate malicious intrusions or dissemination of malicious code; and 3) encouraging the parties to employ risk-based approaches, and enterprises within their jurisdiction to use such approaches.

Article 8.61L of the UKSDEA is the most detailed of the agreements considered, as it extends the USMCA (Article 19.15), although it does not include 2) of the above. It provides for the recognition of the parties and their obligation to encourage juridical persons within their territory to use risk-based approaches, both with detailed provisions.[148]

The EUSDTP (Article 4.2) incorporates some elements of the USMCA (Article 19.15), and of relevant part of the UKSDEA which builds on the USMCA.[149] As the EUSDTP follows the USMCA model, the outcome of the negotiations between the EU and Singapore for a digital trade agreement will be interesting in seeing how the EU reconciles the USMCA model.[150]

In general, cybersecurity measures are said to be increasingly risk-based,[151] and risk-based approaches are being stipulated in trade agreements such as the USMCA. As cybersecurity measures are dynamic processes that are preventive and long-term in nature, and require periodic risk assessments, risk-based approaches are considered more appropriate

---

[147] USMCA Article 19.15: Cybersecurity

1. The Parties recognize that threats to cybersecurity undermine confidence in digital trade. Accordingly, the Parties shall endeavor to:
   (a) build the capabilities of their respective national entities responsible for cybersecurity incident response; and
   (b) strengthen existing collaboration mechanisms for cooperating to identify and mitigate malicious intrusions or dissemination of malicious code that affect electronic networks, and use those mechanisms to swiftly address cybersecurity incidents, as well as for the sharing of information for awareness and best practices.
2. Given the evolving nature of cybersecurity threats, the Parties recognize that risk-based approaches may be more effective than prescriptive regulation in addressing those threats. Accordingly, each Party shall endeavor to employ, and encourage enterprises within its jurisdiction to use, risk-based approaches that rely on consensus-based standards and risk management best practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity events.

[148] On the recognition, for example, it adds the importance of (c) maintaining a dialogue, (d) mutual recognition of basic security standard for consumer IOT devices, and (f) cooperation in R&D, among others. For risk-based approaches, it also imposes an obligation to encourage the use of approaches that rely on open and transparent industry standards (a) to manage cyber security risks and to detect, respond to, and recover from cyber security events and (b) to otherwise improve the cyber security resilience of juridical persons in parties' jurisdictions and their customers.

[149] These elements include: the parties' recognition that cybersecurity incidents and threats undermine confidence in digital trade and that businesses need a secure digital trading environment; the need to build domestic capabilities to identify and mitigate malicious activities and to promote information exchange and cooperation; and the encouragement of businesses to use risk-based approaches that rely on open, transparent and consensus-based standards as well as risk management best practices, given its effectiveness in addressing these threats and minimizing trade barriers.

[150] There is no cybersecurity clause in the narrow sense in the digital trade chapter of the EU-NZFTA.

[151] Meltzer (2019) pp. 1-2.

than "overly prescriptive regulation," which can quickly become outdated.[152] Although risk-based approaches are not clearly defined, at least in the agreements reviewed in this paper, the approaches require "governments, organizations, and businesses to assess the risk of attack, determine potential harm, and develop appropriate measures to reduce the risk or impacts."[153] The USMCA (Article 19.16) also elaborates on the approaches that they "rely on consensus-based standards and risk management best practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity events," which helps one understand the approaches that appear in trade agreements.

In light of the above, the risk-based approaches can be understood as requiring the determination of the measures to be taken on the basis of the existence of a risk, in the same way that SPS measures under the WTO SPS Agreement follow a series of processes whereby the level of acceptable risk is determined on the basis of a risk assessment and the SPS measure is taken to achieve that level. However, confidential nature of cybersecurity may make disclosure of information more difficult than the protection of human, animal and plant life and health, and the same applies to third-party scrutiny.[154] Therefore, cybersecurity measures in trade agreements are currently addressed through provisions on cybersecurity cooperation and through security exceptions clauses that replicate GATT XXI or similar provisions in other WTO agreements. So, the security exceptions will be discussed next.

A well-known security exceptions clause in trade agreements is GATT Article XXI, but the possibility of justifying GATT-inconsistent cybersecurity measures as exceptions under Article XXI is often viewed negatively.[155] The argument is that cybersecurity measures, which are a dynamic process that is generally preventive and long-term in nature, requiring regular risk assessments, do not meet the various conditions set out in GATT Article XXI, such as the need to be taken "in time of... other emergencies in international relations" (GATT Article 21(b)(iii)).[156]

The security exceptions clauses in the trade agreements covered in this paper, with the exception of EUSDTP which yet provides for exceptions clauses, can be divided into two

---

[152] Meltzer (2019) p. 24. The US, EU, Australia and China also favour this approach. For the US, see NIST(2018)p. 3. For the EU, see Directive(EU)2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation(EU)No 910/2014 and Directive(EU)2018/1972, and repealing Directive (EU)2016/1148(NIS 2 Directive). For Australia, see Chang and Liu (2022) p. 195, ft.15. For China, see Meltzer (2019) p. 12.

[153] Meltzer (2019) p. 1; OECD (2015) p. 5; NIST (2018) pp. 4-5. (in particular, 1.2 Risk Management and the Cybersecurity Framework)

[154] Meltzer (2019) p. 26.

[155] E.g., Whitsitt (2023) pp. 8-13; Chang and Liu (2022) pp. 192-193; Meltzer (2019) pp. 20-23.

[156] E.g., Meltzer (2019) pp. 20-23.

types: those that are identical to the CPTPP Article 29.2(Security Exceptions)[157] (CPTPP, USMCA, DEPA, DEA), and those that retain the structure of GATT Article XXI, in particular Article XXI(b) (UKSDEA, EU-UKTCA, RCEP). The former adopts wordings similar to GATT Article XXI, but removes the restriction on measures, by not listing the actions that the party considers necessary for the protection of its essential security interests, as provided for in Article XXI(b) of the GATT, thereby possibly broadening the scope of the exception. The latter, UKSDEA, EU-UKTCA and RCEP, extend the scope of the exception mainly by including additional elements to the list in GATT Article XXI(b).[158] This type seemingly allows more flexibility in justifying cybersecurity measures than GATT Article XXI. Listing permissible actions is more restraining for the parties because the measures to be taken are more limited.

Looking at security exceptions clauses in the context of cybersecurity measures, the provisions of the UKSDEA and the RCEP are particularly noteworthy. The UKSDEA adds to the list of actions "taken...to protect critical public infrastructure (this relates to communications, power or water infrastructure providing essential goods or services to the general public) from deliberate attempts to disable or disrupt it"(Article 16.11(b)(iv)). The RCEP also adds to the same list of actions "taken so as to protect critical public infrastructures including communications, power, and water infrastructures" and "taken in time of national emergency" (Article 17.13(b)(iii) and (iv)).[159] Both provisions appear to encompass measures to protect critical public infrastructure from, for example, cyber-attacks on servers, and are more permissive of cybersecurity measures than GATT Article XXI.[160]

---

[157] CPTPP Article 29.2: Security Exceptions
Nothing in this Agreement shall be construed to:
(a) require a Party to furnish or allow access to any information the disclosure of which it determines to be contrary to its essential security interests; or
(b) preclude a Party from applying measures that it considers necessary for the fulfilment of its obligations with respect to the maintenance or restoration of international peace or security, or the protection of its own essential security interests.

[158] E.g., UKSDEA Article 16.11 Security Exceptions(in relevant part)
Nothing in this Agreement shall be construed to:
…
(b) prevent either Party from taking any action which it considers necessary for the protection of its essential security interests:
(iv) taken in time of war or other emergency in international relations, or to protect critical public infrastructure (this relates to communications, power or water infrastructure providing essential goods or services to the general public) from deliberate attempts to disable or disrupt it;
…

[159] RCEP Article 17.13: Security Exceptions(in relevant part)
Nothing in this Agreement shall be construed:
…
(b) to prevent any Party from taking any action which it considers necessary for the protection of its essential security interests:
(iii) taken so as to protect critical public infrastructures, including communications, power, and water infrastructures;
(iv) taken in time of national emergency or war or other emergency in international relations; or
…

[160] See Whitsitt (2023) pp. 13-16.

Cyber risk is a common threat to all countries interconnected by networks, and therefore requires cooperative responses between countries. At the same time, cybersecurity can be related to national security and so requires a high degree of regulatory autonomy, which can easily lead to disguised trade restrictions, or unlimited measures. The trade agreements examined in this paper take a pragmatic approach in this regard, providing for cooperation on cybersecurity while broadening the scope of exceptions clauses for cybersecurity measures to be allowed under such clauses. However, security exceptions clauses are inherently legally unstable as they are applied on a case-by-case basis. Eventually, more accommodating rules will be needed to reconcile the relationship between trade and cybersecurity.

V-2-3. Response to New "Stakeholder" Involvement

(1) Open Government Data

Since their introduction in the USMCA, open government data provisions have been included in almost all of the agreements examined in this paper, either as is or as developed, with the exception of the RCEP. USMCA Article 19.18 provides for the parties' recognition that public access to and use of data fosters economic and social development, competitiveness and innovation, and the obligation of the parties to endeavor to ensure the easy access by including a machine-readable and searchable format, and to cooperate to identify ways to expand access to and use of government information, including data.

The provisions of the USMCA were reinforced in the DEA and further developed in the EU-UKTCA. DEA Article 27 is almost identical to the USMCA and aims to ensure that government information, including data, is made publicly available in an accessible format, but the manner in which it is made available to the public is more specific.[161] Article 210 of EU-UKTCA further details the manner of public accessibility.[162]

While open government data provisions thus contribute to clarifying and improving the role of government as a holder or provider of data, they have also been criticised for only benefiting companies with the technology and capacity to exploit such data.[163] Given that government data is publicly maintained, it is desirable to ensure that its beneficiaries are not limited and to address such criticisms while promoting the use of government data. An interesting development in this context is that EUSDTP Article 2.2 refers to the possibility of "ex-

---

[161] On specifics: adding "the information is appropriately anonymised, contains descriptive metadata"; and, to the extent practicable, the information is made available in a spatially enabled format with reliable, easy to use and freely available APIs and is regularly updated.

[162] On specifics: (a) in a format to be easily searchable, retrievable, usable, reusable, and redistributable; (b) in a machine-readable and spatially-enabled format; (c) contains descriptive metadata, which is as standard as possible; (d) via reliable, user-friendly and freely available Application Programming Interfaces; (e) regularly updated; (f) not subject to discriminatory use or unnecessarily restrict re-use conditions; and (g) made available for re-use in full compliance with the Parties' respective personal data protection rules.

[163] Streinz (2021) pp. 178-179.

panding the coverage of open government data, such as through engagement and consultation with interested stakeholders." In light of the above criticisms, it is desirable that interested stakeholders will not be limited to data users such as digital platforms.

(2) Stakeholder Engagement

As digital trade and the digital economy affect society as a whole, it is important, as already mentioned, that different stakeholders are involved in the digital trade rule-making process. Notable in this respect are the provisions on stakeholder engagement included in the DEA and the UKSDEA. As their content is identical, the DEA is taken up here. Article 35 of DEA mainly provides for an obligation of the parties to seek opportunities to convene a Digital Economy Dialogue and to promote relevant collaboration efforts and initiatives between them through such a dialogue.

This dialogue would allow for the participation of stakeholders where appropriate, and as may be agreed by the parties, and allow the parties to collaborate with such stakeholders in convening the dialogue. Stakeholders are not defined, but examples include researchers, academics, industry, and others. In this light, RCEP Article 12.6 entitled "Dialogue on Electronic Commerce" provides for the possibility of stakeholder participation in such a dialogue. It seems necessary to monitor how these provisions are applied to ensure compliance.

In terms of stakeholder engagement, digital inclusion in DEPA and UKSDEA (see below) also provides for an opportunity for stakeholder consultation. It would be ideal to include both, as in UKSDEA.

V-2-4. Response to Digital Divide

(1) Digital Inclusion

Of the agreements examined in this paper, only the DEPA and the UKSDEA include digital inclusion.[164] Although digital inclusion is not defined, DEPA takes up, for example, "participation of women, rural populations, low socio-economic groups and Indigenous Peoples in the digital economy" as relevant matters, indicating that these are at least included (Article 11.1.3). In addition, the UKSDEA mentions the digital divide between countries (Article 8.61P).

The provisions of the DEPA have been further developed in the UKSDEA. DEPA Article 11.1 provides for the parties' recognition of the importance of digital inclusion and of expanding and facilitating digital economy opportunities by removing barriers, including by enhancing cultural and people-to-people links, and improving access for women, rural pop-

[164] EUSDTP Section 5 (Cooperation on Digital Trade) provides for similar elements, including addressing barriers to the participation in the digital economy faced by women and other low socio-economic groups, and supporting micro, small and medium-sized enterprises.

ulations and low socio-economic groups. It also obliges the parties to cooperate on matters related to digital inclusion with the illustration thereof, and that such cooperation activities may be carried out through the coordination of the parties' respective agencies, enterprises, labour unions, civil society, academic institutions and NGOs, among others. Article 8.61P of the UKSDEA enhances the relevant provisions of the DEPA by providing more detailed recognition of the parties and specific examples of the parties' obligation to cooperate than in the DEPA, by providing for the parties' recognition of the digital divide and their obligation to endeavour to strengthen cooperation, and ways to address it, and by adding a new obligation to participate actively in international fora such as the WTO to promote initiatives for advancing digital inclusion in digital trade.

Interestingly, the DEPA and the UKSDEA acknowledge the importance of digital inclusion in general, not just within the parties' jurisdictions, and set out obligations of the parties to cooperate, with examples of cooperations activities to this end and the explicit involvement of civil society and other stakeholders. It would be important to monitor the application of these provisions to ensure compliance, together with stakeholder engagement.

(2) SMEs and Developing Countries

In terms of the digital divide, the lack of capacity in Small and Medium-sized Enterprises (SMEs) and developing countries is of particular concern.[165] FTAs may include chapters on SMEs and development, but only DEPA, DEA and UKSDEA of the agreements reviewed in this paper address these issues in the context of digital trade. In particular, DEPA Module 10 (SME cooperation) is detailed and imposes obligations on parties to cooperate, share information and engage in dialogue in order to enhance trade and investment opportunities and promote jobs and growth for SMEs in the digital economy. It is noteworthy that a number of provisions on SME support have been included.[166]

On the digital divide between developed and developing countries, digital inclusion provisions can be part of the response to such a challenge. For example, the DEPA (Article 11.1), while not specifically referring to developing countries, lists "developing programmes to promote participation of all groups in the digital economy" as one of the cooperation activities (Article 11.1.3.d). In addition, as already noted, the UKSDEA (Article 8.61P) refers to the digital divide between countries. This is not common in other agreements and is also sugges-

[165] WTO (2018) Section B.

[166] Examples include: the parties' recognition of the fundamental role of SMEs in the digital economy and the integral role of the private sector in the SMEs-related cooperation (Article 10.1 General Principles); obligation of the parties to cooperate to exchange relevant information and to encourage the participation by the parties' SMEs in platforms helping SMEs (Article 10.2 Cooperation to Enhance Trade and Investment Opportunities for SMEs in the Digital Economy); obligation of the parties to establish or maintain its own website for the provision of information and the regular review thereof (Article 10.3 Information Sharing); and obligation of the parties to convene a Digital SME Dialogue, possibly with the participation of the private sector, NGOs, academic experts and other stakeholders from each party, possibly using the input therefrom (Article 10.4 Digital SME Dialogue).

tive in that the scope of application is not limited to the jurisdictions of the parties.

Consideration for development is also reflected in the transitional period given to developing country parties to implement the obligations of the agreements. This has been the case in agreements where developing countries are parties, such as CPTPP, USMCA and RCEP.[167]

V-2-5. Response to Other Issues

(1) AI, Digital ID, "Tech" Issues

In addition to the issues discussed so far, an interesting aspect of the agreements examined in this paper is that they contain provisions on novel issues that may further extend the scope of trade agreements. Common to DEPA, DEA and UKSDEA are, among others, AI, digital ID and "Tech" issues—Fintech, Regtech and Lawtech.

Provisions on AI were introduced in the DEPA (Article 8.2) and then gradually developed in the DEA (Article 31) and the UKSDEA (Article 8.61R). The main common elements are: 1) recognition by the Parties, including, of the importance of AI; 2) development of AI governance frameworks with reference to ethical elements; and 3) consideration of internationally recognised principles or guidelines in the development of such frameworks.[168] On this point, it is said that there is no universally agreed definition of AI[169] and AI is not defined in these agreements, either.

AI has attracted more interest than ever before, from around early 2023, particularly with the rapid proliferation of so-called generative AI, such as ChatGPT, and the need for discipline is being discussed internationally. So far, AI has not been a main subject in FTAs, but with regulations being introduced in many countries, it is likely to be one of the issues that will be addressed in FTAs in the future. In doing so, in addition to the lack of common definitions mentioned above, the focus is likely to be on the relationship between national regulations and trade restrictiveness on the one hand, and the permissible scope of regulation on the other, as with current data-related regulations. Furthermore, as the provisions on the AI governance frameworks refer to the ethical elements, such elements could also be discussed

---

[167] The CPTPP and the USMCA also have SMEs chapters to support SMEs in general, but not specifically for digital trade.

[168] The EUSDTP also covers AI and refers to the elements 1) to 3).

[169] E.g., CRS (2021) pp. 1-2. On this point, the OECD updated its AI principles in May 2024, originally adopted in 2019, which includes the definition of "AI system." <https://www.oecd.org/newsroom/oecd-updates-ai-principles-to-stay-abreast-of-rapid-technological-developments.htm> The EU AI Act is worth mentioning in terms of national legislation defining AI. This Act was approved by European Parliament in March 2024 and was endorsed by the European Council in May 2024. Article 3 of the Act defines the "AI system" as a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments." This definition is very similar to that of the updated OECD Principles. On EU Parliament adoption, see EU Parliament press release, "Artificial Intelligence Act: MEPs adopt landmark law"
<https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law> On European Council approval, see European Council press release, 21 May 2024, "Artificial intelligence (AI) act: Council gives final green light to the first worldwide rules on AI" <https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/>

in the context of trade agreements. This in turn suggests that the non-trade issues covered by FTAs could be further extended.

For digital ID, the DEPA introduced the relevant provisions, which were then strengthened by the DEA, followed by the UKSDEA. The DEPA (Article 7.1, Digital ID), recognising, inter alia, that the implementation of, and legal approaches to digital ID may differ between parties, obliges the parties primarily to endeavour to promote the interoperability with illustrations of the ways to achieve this, such as the establishment of common standards. However, it does not preclude the adoption or maintenance of measures to achieve LPPO, even if such measures are inconsistent with such obligations. The DEPA does not define digital ID, but according to the OECD (2023), for example, it is referred to as "a set of electronically captured and stored attributes and/or credentials that can be used to prove a feature, quality, characteristic, or assertion about a user, and, when required, support the unique identification of that user."[170] The DEA (Article 29) is similar to the DEPA (Article 7.1) in this respect, but is strengthened in the following respects: 1) obliging the parties to pursue the development of mechanisms to promote compatibility of different legal and technical approaches to digital ID between the parties; 2) obliging the parties to endeavour to facilitate initiatives to promote such compatibility; and 3) not providing for LPPO "exceptions" as the DEPA does.[171]

In terms of "Tech" related provisions, Fintech was covered by the DEPA, then Regtech by the DEA, and Lawtech was added to these in the UKSDEA.[172] The main content of these provisions is cooperation between the parties. These terms are explained in these agreements: Fintech as "the use of technology to improve and automate the delivery and use of financial services" (DEA Article 1.r); Regtech as "the use of information technology to improve and manage compliance with regulatory processes" (DEA Article 1.x); and Lawtech as "technologies that aim to support, supplement or replace traditional methods for delivering legal services." (UKSDEA Article 8.57.r)

(2) Submarine Cable Systems

Stable infrastructure is essential for cross-border data transfer, and submarine cable systems are one such infrastructure. Trade agreements may contain provisions on submarine cable systems, which tend to be pro-competitive in nature, such as requiring a party to ensure

---

[170] OECD (2023), *Recommendation of the Council on the Governance of Digital Identity*, OECD/ LEGAL/0491, p. 6.

[171] The DEA in addition has MOUs that provide for practical means of cooperation between the parties, digital identity being one of them. Other areas covered are: data innovation; AI, trade facilitation; electronic invoicing; electronic certification cooperation for agricultural products; and personal data protection.

[172] However, the UKSDEA only provides for cooperation between the parties on Fintech and Regtech. "Fintech and Regtech" are referred to as "activities which involve the improved use of technology across financial services" in the UKSDEA for the purposes of the relevant article (Article 8.53.2 ft.2).

that its operators of submarine cable systems or landing stations provide access on reasonable and non-discriminatory terms to operators from the other parties. The agreements examined in this paper contain the relevant provisions from a pro-competitive perspective, namely the CPTPP (Article 13.15), the USMCA (Article 18.13) and the RCEP (Annex 8-B, Article 18).

On the other hand, the relevant provisions of the DEA and the UKSDEA are novel and noteworthy because they include an infrastructure stability perspective. The DEA (Article 22, Submarine Telecommunication Cable Systems (STCS)) focuses on the importance of submarine telecommunication cable systems as infrastructure and the need to ensure infrastructure stability, including their installation and operation, with very detailed provisions on the expeditious and efficient installation, maintenance and repair of these systems ("Operational Elements"), as well as on the possibilities for consultations regarding the measure which creates a material impediment to the Operational Elements, and the obligations of the parties to enter into consultations, if requested. In particular, it provides for the parties' recognition of the importance of submarine telecommunications cable systems and their expeditious and efficient Operational Elements to telecommunications connectivity. It then sets out the obligations of a party to endeavour to ensure that a person of the other party who operates, owns or controls submarine telecommunications systems has flexibility to choose suppliers of Operational Elements, including from a non-Party, and that procedural aspects are warranted[173] when requiring a permit for a vessel registered outside the territory to undertake Operational Elements of the submarine telecommunications cable system of which a person of the other party operates, owns or controls. Other obligations on a party are to endeavour to mitigate the risk of damage to STCS operated, owned or controlled by a person of the other party, with the illustrations of the means thereof, including making information available on the location of STCS to inform mapping and charting.

The UKSDEA (Article 8.38, Submarine Cable Landing Stations (SCLS) and Cable Systems (SCS)) mainly provides for the following elements: the recognition by the parties of the importance of the expeditious and efficient Operational Elements of SCLS and SCS; the obligation of a party to ensure access to SCLS and SCS on reasonable, non-discriminatory and transparent terms and conditions when a supplier is authorized to operate SCS as a public telecommunication service; allowing a party to mitigate the risk of damage to SCLS and SCS in its territory where a person of the other party operates, owns or controls; and the obligations of the parties to endeavour to cooperate on SCLS and SCS.

[173] On specifics in relation to such permit: (a) publication of the activities subject to permit; (b) publication of the requirements and procedures; (c) publication of the assessment criteria; (d) reasonable, objective and impartial administration of the application and renewal procedures; (e) notification of the decision to the applicant within a reasonable period; (f) sufficient duration for required installation, maintenance or repairs of submarine telecommunications cable systems after the grant of such permit; and (g) reasonableness and transparency of the fees and limitation of the fees to the approximate cost of services rendered by the competent body (Article 22.2).

While the DEA places more emphasis on the infrastructure stability perspective, such as the importance of submarine telecommunication cable systems and their Operational Elements, the UKSDA adds the pro-competitive perspective by requiring the parties to ensure access to SCLS and SCS. The provisions relating to submarine cable systems do not seem to attract as much attention at present as the data-related provisions in the context of digital trade, but they are likely to become more important in the future as the volume of cross-border data flows is expected to continue to increase.

(3) Other Novel Issues

In addition to the issues discussed in the previous sections, the EUSDTP, the most recent trade principles reviewed in this paper, also covered the protection of non-personal data (Article 2.1.5) and government access to personal data held by the private sector (Article 2.1.7). Both are relatively new issues. The OECD has just adopted its first recommendation on government access in 2022,[174] which describes it as "government access to and processing of personal data in the possession or control of private sector entities when governments are pursuing law enforcement and national security purposes within their respective territories in accordance with their national legal framework, including situations where countries have the authority under their national legal framework to mandate that private sector entities provide data to the government when the private sector entity or data are not located within their territory."[175] These may also become key issues for digital trade rules in the future.

VI. Conclusions

This paper has discussed the four main challenges that digital trade poses to traditional international trade (five perspectives if the "response to other issues" section is included) and the response to these challenges through trade agreements, with a particular focus on trade agreements of "rule-maker" countries of digital trade rules, given the limitations of the WTO's response. The findings are presented below.

The first is the interaction between trade agreements in the evolution of the digital trade provisions. The agreements covered in this paper can be broadly grouped into three patterns in terms of digital trade: the Asia-Pacific pattern (CPTPP, USMCA, DEPA, DEA, UKSDEA), the EU pattern (EU- UKTCA, EUSDTP) and others (RCEP). In the Asia-Pacific pattern, the CPTPP was built on the SAFTA, which led to the USMCA, the DEPA and the DEA. However, all of them have had an impact on the UKSDEA. As already mentioned, the UKSDEA

[174] OECD, *Declaration on Government Access to Personal Data Held by Private Sector Entities*, OECD/ LEGAL/0487. <https://www.ppc.go.jp/files/pdf/government_access_jp.pdf>

[175] Ibid., p.6.

stands out for its novelty and inclusiveness, incorporating some of the best aspects of DEPA, such as digital inclusion. At the same time, the UKSDEA builds on and enhances the cybersecurity provisions of the USMCA. It also covers stakeholder participation, provisions on submarine cable systems, including from an infrastructure stability perspective, restrained security exceptions compared to other agreements such as the CPTPP and the USMCA, and positive attitudes on emerging issues, such as AI, Fintech, Regtech, and Lawtech.

On the other hand, the EU, when concluding FTAs, has traditionally covered e-commerce under the chapter on "Trade in Services, Establishment and the E-commerce."[176] However, this appears to be changing with the introduction of a separate chapter on digital trade in the EU-UKTCA and the EU-NZFTA.[177] While some features of the new chapter differ from the Asia-Pacific pattern, such as the unique structure of the data-related provisions, the interaction between the two patterns can be observed, as the EU-UKTCA develops open government data provisions based on the USMCA, and the EUSDTP includes AI provisions with similar elements to the DEPA and others.

While it has been noted that digital trade provisions in FTAs have evolved over time, this study shows that the pioneering agreements of "rule-maker" countries have interacted to refine and shape digital trade rules. At the same time, it finds that new elements are emerging in trade agreements, such as provisions on submarine cable systems from an infrastructure stability perspective, AI and "Tech" related provisions, as well as novel issues including government access and non-personal data. In light of these developments, the evolution and sophistication of digital trade provisions can be expected to continue in the future. What this paper has presented is, of course, only a snapshot of the moment. However, the snapshot is suggestive of future rule-making in digital trade, as pioneering agreements or rules are proposed by "rule-maker" countries, and they appear to be competing for influence over such rule-making processes.

Second, this study found that digital trade has broadened the scope of trade agreements and their implications. The scope of "trade-relatedness" in digital trade rules appears to be broader than before, perhaps because digitalisation affects the economy and society more generally. This can be seen in provisions that are not necessarily directly "trade-related" and that substantially address "non-trade concerns", which are addressed by exceptions clauses in the WTO agreements, such as the protection of personal data or cybersecurity. Such provisions have already increased particulary in the environment and labor chapters in FTAs, but the development of digital trade seems to have reinforced this trend.[178]

---

[176] Wu (2017), p.9.

[177] EU-NZFTA was signed in July 2023.

[178] Digital trade is not the only cause of this, of course, but the rise of non-trade issues such as environment and labour, and the emergence of states, such as China, that more closely link security and economic or market issues, are also relevant. On the rise of non-trade issues, see Matsushita and Iino (2021), pp. 4-6.

It can be seen as integrating "non-trade concerns" into trade rules, and can be valued as seeking a balance between trade and non-trade concerns, or market and non-market mechanisms, that ultimately makes the overall rules more sustainable.[179] However, as trade agreements go deeper into "non-trade concerns," the "right to regulate" of the parties is more emphasized, while at the same time more attention is given to "interoperability," "compatibility," or "cooperation" between the different approaches or systems.

Third, which is also related to the second point, is the growing presence of the "right to regulate" in digital trade rules and its increasing prevalence in advanced trade agreements. One view of the "right to regulate" in the WTO context is that it is "materialized as a discretion of a Member to pursue policy objectives it deems important, or the freedom to determine an acceptable level of risk within its jurisdiction."[180]

In the WTO agreement, however, the "right to regulate" itself does not have the same presence as it does in the FTAs examined in this paper. It is mentioned in the preamble of the GATS, but not in the preamble of the Marrakesh Agreement Establishing the WTO, unlike the preambles of the agreements examined in this paper, which make explicit reference to it. The concept of the "right to regulate" is, of course, reflected in the WTO agreements. The exceptions clauses such as GATT Articles XX and XXI and the Preamble to the TBT Agreement (6th recital) have been interpreted by the AB as reflecting or confirming the existence of such a right,[181] and the SPS Agreement also provides for the "right" of Members to adopt certain SPS measures.[182]

On the other hand, the "right to regulate" found in the FTAs examined in this paper is increasing its presence, together with the concepts such as LPPO, which expresses the policy space of the parties. However, its content is not so clear, at least in the respective agreements reviewed in this paper. The concern is that the "right to regulate" and LPPO or LPPO-like concepts may erode the rules to the point where they become meaningless.

In this respect, if regulatory autonomy is emphasised in this way through the "right to regulate" in the context of digital trade, the involvement of various stakeholders in the rule-making process for digital trade will be necessary to ensure its legitimacy and fairness in the light of the far-reaching impact of digitalisation on society, and even more so in the post rule-making review phase.

From this perspective, provisions on stakeholder participation seem to be of particular

---

[179] However, the perspective of trade and non-trade, or of market and non-market mechanism, can itself be taken as placing focus on economic interests.

[180] So (2019), p. 2.

[181] Appellate Body Report United States – Measures Affecting the Production and Sale of Clove Cigarettes WT/DS406/AB/R, para.95; Appellate Body Reports, European Communities – Measures Prohibiting the Importation and Marketing of Seal Products, WT/DS400/AB/R / WT/DS401/AB/R, para.5.125.

[182] SPS Agreement, Article 2.1.

importance, but fourthly, even in the pioneering agreements of the 'rule-maker' countries reviewed in this paper, only a few examples of stakeholder participation were found. If the free flow of data is an aspiration, it is also necessary to consider the environment to ensure this, but only a few examples were found on the digital divide, a challenge in this regard. These aspects should be better addressed in digital trade rules.

References

Ishii, K. (2017), *The revised version of Present and the Future of Laws on the Protection of Personal Data: The World Surroundings and the Future Prospect in Japan*, Keiso Publishing. [in Japanese]

Kimura, M. (2022),"Kinji No Tsūshokyotei Ni Mirareru Kinyu Service Bunya Ni Okeru Data Kanren No Kiritsu (Data-Related Provisions in the Financial Services Sector in Recent Trade Agreements)", *Kokusai Shōji Hōmu (Journal of the Japanese Institute of International Business Law)*, Vol. 50, No. 12, pp. 1565- 1570. [in Japanese]

Matsushita, M. and A. Iino (2021), "Gendai Kokusaitsūshōhō System No Panorama (A Panoramic View of the International Trading System)", *Kokusai Shōji Hōmu (Journal of the Japanese Institute of International Business Law)*, Vol. 49, No. 99, pp. 1-13. [in Japanese]

REUTERS (digital, June 3, 2022) "Sony Ga Shinkaisha Setsuritsu, Eisei Reiza Hikari Tsushin Sochi Wo Seizo He (Sony to Establish New Company for Satellite Laser Optical Communications Equipment)",
<https://jp.reuters.com/article/space-sony-group-idJPKBN2NJ24P> [in Japanese]

So, H. (2019), *Trade liberalization and Regulatory Autonomy: the Balance Established in* WTO *law*, The University of Tokyo Press (UTP). [in Japanese]

The Asahi Shimbun (digital, October 11, 2022), "Space X no Eisei Net Tsushin 'Starlink', Nihon Demo Service Kaishi (SpaceX's Starlink Satellite Net Communications Service Launched in Japan)" [in Japanese]
<https://www.asahi.com/articles/ASQBC6RCBQBCULFA026.html> [in Japanese]

The Nikkan Kogyo Shimbun (November 23, 2022), "Space X Ga Nihon De 'Starlink'Kaishi, 'Rival Yorimo Yuri Na Jokyo' No Riyu (SpaceX Launches 'Starlink' in Japan, Why It Has 'an Advantage over Its Rivals')",
<https://newswitch.jp/p/34697> [in Japanese]

Aaronson, S., and P. Leblond (2018), "Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO", *Journal of International Economic Law*, Vol. 21 No. 2, pp. 245-272.

Burri, M. (2021), "Chapter 1 Data Flows and Global Trade Law", in M. Burri (ed.), *Big Data and Global Trade Law*, Cambridge University Press, pp. 11-41.

Burri, M. (2022), "Chapter 28 Privacy and data protection", in D. Bethlehem, D. McRae,

Chang, L. Y.-C., and H.-W. Liu (2022), "Chapter 8 Ensuring Cybersecurity for Digital Services Trade", in J. W. Kang, et al. (Asian Development Bank), *Unlocking the Potential of Digital Services Trade in Asia and the Pacific*, pp. 184-204.

Congressional Research Service (2021), *Artificial Intelligence: Background, Selected Issues, and Policy Considerations*, R46795. Ver.3. <https://crsreports.congress.gov/product/pdf/R/R46795>

Damme, I. V. (2019), "Chap 16 Understanding the Choice for Evolutionary Interpretation", in G. Abi-Saab, Georges Abi-Saab, and K. Keith, G. Marceau, and C. Marquet (eds.), *Evolutionary Interpretation and International Law*, Bloomsbury, pp. 171-180.

Elsig, M., and S. Klotz (2021), "Chapter 2 Data Flow-Related Provisions in Preferential Trade Agreements Trends and Patterns of Diffusion", in M. Burri (ed.), *Big Data and Global Trade Law*, Cambridge University Press, pp. 42-62.

Gagliani, G. (2020), "Cybersecurity, Technological Neutrality, and International Trade Law", *Journal of International Economic Law*, Vol. 23, No. 3, pp. 731-738.

Gleason, T., and C. Titi (2022), "The Right to Regulate", Academic Forum on ISDS Concept Paper, 2022/2 https://ssrn.com/abstract=4255605

González, L. J., and M. Jouanjean (2017), "Digital Trade: Developing a Framework for Analysis", OECD Trade Policy Papers, No. 205, OECD Publishing, Paris.

IMF, OECD, UN, and WTO (2023), *Handbook on Measuring Digital Trade: 2nd Edition*, WTO.

Inside US Trade (2023), "New WTO text on E-Commerce Shows Divisions over Privacy, Data Flows", August 14, 2023.

Inside US Trade (2024), "Industry groups: WTO e-commerce JSI needs lasting moratorium", April 24, 2024.

McKinsey Global Institute (2016), *Digital Globalization: The New Era of Global Flows*, McKinsey & Company.

Meltzer, J. P. (2019), "Cybersecurity and Digital Trade: What Role for International Trade Rules?", *Global Economy and Development Working Paper 132*, the Brookings Institution.

Mitchell, A. D. (2008), *Legal Principles in WTO Disputes*, Cambridge University Press.

Monteiro, J.-A., and R. Teh (2017), "Provisions on Electronic Commerce in Regional Trade Agreements", WTO Working Papers ERSD- 2017-11.

National Institute of Standards and Technology (NIST) (2018), *Framework for Improving Critical Infrastructure Cybersecurity: Version 1.1*, NIST. <https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf>

Neufeld, R. and I. Van Damme (eds.) (2022), *The Oxford Handbook on International Trade*

Law, 2nd ed., Oxford University Press, pp. 745-768.

OECD (2015), *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*, OECD Publishing, Paris.

OECD (2019), *An Introduction to Online Platforms and Their Role in the Digital Transformation*, OECD Publishing, Paris.

OECD (2022), *Cross-border Data Flows: Taking Stock of Key Policies and Initiatives*, OECD Publishing, Paris.

OECD (2023), "Moving Forward on Data Free Flow with Trust: New Evidence and Analysis of Business Experiences", OECD Digital Economy Papers, No. 353, OECD Publishing, Paris.

Peng, S., C. F. Lin., and T. Streinz (2021), "Artificial Intelligence and International Economic Law: A Research and Policy Agenda", in S. Peng, C. F. Lin, and T. Streinz (eds.), *Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration*, Cambridge University Press, pp. 1-26.

Peng, S. (2022), "Chapter 29 Digital Trade", in D. Bethlehem, D. McRae, R. Neufeld, and I. Van Damme (eds.), *The Oxford Handbook on International Trade Law, 2nd ed.*, Oxford University Press, pp. 771-789.

REUTERS (digital) December 2, 2022 "Arctic Data Cable Linking Europe to Japan Secures First Investment" <https://www.reuters.com/technology/arctic-data-cable-linking-europe-japan-secures-first-investment-2022-12-02/>

Shaffer, G. (2021), "Trade Law in a Data- Driven Economy: The Need for Modesty and Resilience" in S. Y. Peng, C. F. Lin, and T. Streinz (eds.), *Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration*, Cambridge University Press, pp. 29-53.

Streinz, T. (2021), "International Economic Law's Regulation of Data as a Resource for the Artificial Intelligence Economy" in S. Y. Peng, C. F. Lin, and T. Streinz (eds.), *Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration*, Cambridge University Press, pp. 175-192.

The Economist (digital) May 6, 2017 "The World's Most Valuable Resource Is No Longer Oil, But Data" <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>

Whitsitt, E. (2023), "International Trade Law and Cybersecurity: Balancing Market- Oriented and Domestic State Regulation" in T. Ishikawa, and Y. Kryvoi (eds.), *Public and Private Governance of Cybersecurity: Challenges and Potential*, Cambridge University Press (Forthcoming) <https://ssrn.com/abstract=4309960>

WTO (2018), *World Trade Report 2018: The Future of World Trade: How Digital Technologies are Transforming Global Commerce*, WTO.

Wu, M. (2017), "Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System", RTA Exchange, International Centre for Trade and Sustainable Development (ICTSD) and the Inter-American Development Bank (IDB) <www.rtaexchange.org/>

Zhang, S. (2021), "Protection of Cross-Border Data Flows Under International Investment Law", in J. Chaisse, L. Choukroune, and S. Jusoh (eds.), *Handbook of International Investment Law and Policy*, Springer, pp. 1-23.

Appendix

EC: Electronic Commerce DT: Digital Trade DE: Digital Economy	CPTPP 2018 Chapter 14 EC	USMCA 2018/2020 Chapter 19 DT	DEPA 2020/2021	DEA (SAFTA) 2020 Chapter 14 DE	UKSDEA(UKSFTA) 2022 Chapter 8 Section F DT and DE	EU-UKTCA 2020/2021 Title III DT	EUSDTP 2023 *8	RCEP 2020/2022 Chapter 12 EC
Cross-Border Data Transfer	○	○	○ (similar to CPTPP)	○ (CPTPP/DEPA -like)	○ (DEA -like)	○	○	○
Financial services (FS)	○ (FS Chapter)	○ (FS Chapter)	×	○	○ (FS Section)	<not excluded>	<not referred>	○ (Annex to FS Chapter)
LPPO “exceptions”	○	○	○	○	○	<right*2>	<not referred>	○
Prohibition of Localization Requirement	○	○	○ (similar to CPTPP)	○ (CPTPP/DEPA -like)	○ (DEA -like)	○ (prohibition of four categories)	○	○
Financial services (FS)	×	○ (FS Chapter)	×	○	○ (FS Section)	<not excluded>	<not referred>	×
LPPO “exceptions”	○	×	○	○	○	<right*2>	○	○
“Right to Regulate” in Preamble	○ *1	○ *1	○ *1	○ *1	△ *11	○	○	○
Illustration of LPPO/LPWO in preamble	○ *3	○ *3	×	○ *3	○ (LPPO)*11	○ (LPPO)	×	×
Provisions on “right to regulate”	×	×	×	×	△ *11	○ /illustrating LPO	×	×
Personal Information Protection Obligation to adopt/maintain legal framework	○	○	○	○ (USMCA rein-roced)	○ (DEA + USMCA)	provision on protection of personal data/ privacy	reference to data protection	○
Consideration of international principles and guidelines	○ (non mandatory)	○ (non mandatory)	○ (mandatory)	○ (USMCA rein-roced, mandato-ry)	○ (DEA + USMCA, mandatory)			○ (mandatory)
Explicit reference to OECD/APEC	×	○	×	○ (USMCA rein-roced)	×			×
Cybersecurity Recognition of parties	○	○	○	○ *9	○ (USMCA enhanced)	△ (cooperation)	○	○
Capacity improvement of the authority	×	○	△ (Recogni-tion)	×	△ (recognition)	△ (cooperation)	○	×
Risk-based approaches	×	○	×	×	○ (USMCA enhanced)	△ (cooperation)	○	×
Security Exceptions	CPTPP type	CPTPP type*4	CPTPP type*4	CPTPP type*4	GATT Art.XXI type*5	GATT Art.XXI type*5	<not stipulat-ed>	GATT Art. XXI type*5

EC: Electronic Commerce DT: Digital Trade DE: Digital Economy	CPTPP 2018 Chapter 14 EC	USMCA 2018/2020 Chapter 19 DT	DEPA 2020/2021	DEA (SAFTA) 2020 Chapter 14 DE	UKSDEA(UKSFTA) 2022 Chapter 8 Section F DT and DE	EU-UKTCA 2020/2021 Title III DT	EUSDTP 2023 *8	RCEP 2020/2022 Chapter 12 EC
Open Government Data	×	○	○	○ (USMCA rein-forced)	○ (DEA -like)	○ (USMCA en-hanced)	○	×
Stakeholder Engagement	×	×	×	○	○ (DEA -like)	×	×	△ *6
Digital Inclusion (DI)	×	×	○	×	○ (DEPA enhanced)	×	×	×
Development	△ *7	△ *7	○ (DI)*10	○	○ (DI)*10	×	×	△ *7
SMEs	×	×	○	○	○	×	×	×
Digital ID	×	×	○	○ (DEPA rein-forced)	○ (DEA -like)	×	×	×
AI Recognition of parties	×	×	○	○	○	×	○	×
AI governance framework	×	×	○	○	○	×	○	×
Consideration of international principles and guidelines	×	×	○	○	○	×	○	×
Cooperation	×	×	×	○	○	×	×	×
Fintech	×	×	○	○	○ (FS Section)	×	×	×
Regtech	×	×	×	○	○ (FS Section)	×	×	×
Lawetech	×	×	×	×	○	×	×	×

Source: Created by the author based on the respective agreements. LPPO: legitimate public policy objective; LPWO: legitimate public welfare objective; LPO: legitimate policy objective.

*The year below each agreement indicates the year of signature/entry into force (no distinction indicates signed and entered into force in the same year). The chapters below each agreement indicate the main chapters examined.

*1: "inherent right...to regulate" is stipulated. *2: EU-UKTCA stipulates the "right to regulate" (see also main text). *3: LPWO is illustrated. *4: CPTPP type means identical to CPTPP (see also main text).

*5: GATT Article XXI type means the list in GATT Article XXI(b) is maintained with some additions and/or modifications (see also main text). *6: Referred to in the Article on E-commerce Dialogue. *7: Transition period provided. *8: Covering protection of non-personal data and government access to personal data held by private companies (see also main text). *9: MOU on cooperation for cybersecurity exists between Australia and Singapore. *10: DI means that it is stipulated in the article on DI. (see also main text). *11: UKSFTA Article 8.1 (Objective and Scope) stipulates that each party retains the “right to regulate” with the illustration of LPPO in the preamble.