Forthcoming in: David Collins and Michael Geist (eds) *Handbook on Digital Trade* (Cheltenham: Edward Elgar, 2023).

DIGITAL TRADE RULEMAKING IN FREE TRADE AGREEMENTS

Mira Burri[*]

The chapter seeks to provide a better understanding and contextualization of the highly dynamic field of digital trade rulemaking driven by free trade agreements (FTAs). The analytical lens is directed in particular towards the more recent and advanced models of digital trade rulemaking, such as those under the Comprehensive and Progressive Agreement for Transpacific Partnership (CPTPP) and the United States Mexico Canada Agreement (USMCA), as well as those endorsed by dedicated digital economy agreements (DEAs). The chapter also covers the European Union's (EU) new generation of trade deals and looks at the Regional Comprehensive Economic Partnership (RCEP), as the first agreement with digital trade provisions that includes China, so as to give a sense of the dynamic governance environment on issues of digital trade. The chapter identifies points of convergence and divergence in the FTA landscape of digital trade rules across issues and stakeholders, sketches emerging trends and in conclusion provides an outlook on future developments.

I. INTRODUCTION

'Electronic commerce' or 'digital trade',[1] as it is now commonly referred to, is not an entirely new topic in the domain of international economic law. Indeed, the membership of the World Trade Organization WTO) initiated already in 1998 a Work Programme[2] to address the implications of the Internet that could potentially lead to adjustments in the existing rules for trade in goods, trade in services and intellectual property rights (IP) protection. Yet, this effort was largely unsuccessful for two decades and in the meantime, digital trade as practice and as a subject of regulation has entered into an entirely new phase. On the one hand, this has been spurred by the progressively advancing digitization of economies and societies as a whole as well as by the more recently emerged importance of data;[3] on the other hand, the surge in digital trade

[*] Professor of International Economic and Internet Law, University of Lucerne, Switzerland. Contact: mira.burri@unilu.ch. The support of the European Research Council under Consolidator Grant 101003216 is gratefully acknowledged.

[1] The OECD has pointed out that, while there is no single recognized and accepted definition of digital trade, there is a growing consensus that it encompasses digitally-enabled transactions of trade in goods and services that can either be digitally or physically delivered, and that involve consumers, firms, and governments. Critical is that the movement of data underpins contemporary digital trade and can also itself be traded as an asset and a means through which global value chains are organized and services delivered. See Javier López González and Marie-Agnes Jouanjean, 'Digital Trade: Developing a Framework for Analysis', *OECD Trade Policy Papers* 205 (2017).

[2] WTO, Work Programme on Electronic Commerce, WT/L/274, 30 September 1998.

[3] See e.g. James Manyika et al., *Big Data: The Next Frontier for Innovation, Competition, and Productivity* (Washington, DC: McKinsey Global Institute 2011); Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (New

rulemaking, which in this chapter covers both hard and soft rules creation,[4] can be linked to the multiple new issues that the data-driven economy has raised – some of which, such as those in the area of personal data protection, demand urgent regulatory responses.[5]

The chapter is set against this background and seeks to provide a better understanding and contextualization of the highly dynamic field of digital trade rulemaking driven by free trade agreements (FTAs). The new rules found in bilateral and regional FTAs not only compensate for the lack of developments in the multilateral forum of the WTO (at least so far)[6] but effectively create a comprehensive, albeit fragmented, governance framework for the data-driven economy. The chapter's analytical lens is directed in particular towards the more recent and advanced models of digital trade rulemaking, such as those under the Comprehensive and Progressive Agreement for Transpacific Partnership (CPTPP) and the United States Mexico Canada Agreement (USMCA), as well as those endorsed by dedicated digital economy agreements (DEAs). The chapter then covers the European Union's (EU) new generation of trade deals, in particular the post-Brexit agreement with the United Kingdom (UK), the agreement with New Zealand, and the currently negotiated deals with Australia and Tunisia, and looks at the Regional Comprehensive Economic Partnership (RCEP), as the first agreement with digital trade provisions that includes China, so as to give a sense of the dynamic governance environment on issues of digital trade. Subsequently, the chapter identifies points of convergence and divergence in the FTA landscape of digital trade rules, sketches some emerging trends and in concluding provides an outlook on future developments.

II. The FTA Landscape of Digital Trade Rulemaking

A. Overview

The regulatory environment for digital trade has been shaped by FTAs. Out of the 360 plus FTAs entered into between 2000 and 2022, 203 contain provisions relevant for

York: Eamon Dolan/Houghton Mifflin Harcourt, 2013); Nicolaus Henke et al., *The Age of Analytics: Competing in a Data-Driven World* (Washington, DC: McKinsey Global Institute 2016); WTO, *World Trade Report 2018: The Future of World Trade: How Digital Technologies Are Transforming Global Commerce* (Geneva: World Trade Organization, 2018).

[4] See e.g. Kenneth W. Abbott and Duncan Snidal, 'Hard and Soft Law in International Governance', *International Organization* 54:3 (2000), 421–456; Gregory C. Shaffer and Mark A. Pollack, 'Hard vs. Soft Law: Alternatives, Complements, and Antagonists in International Governance', *Minnesota Law Review* 94 (2010), 706–799.

[5] See e.g. Mira Burri, 'Interfacing Privacy and Trade', *Case Western Journal of International Law* 53 (2021), 35–88; Anupam Chander and Paul M. Schwartz, 'Privacy and/or Trade', *University of Chicago Law Review* 90:1 (forthcoming 2023), available at: http://dx.doi.org/10.2139/ssrn.4038531

[6] For an analysis of the WTO relevance to digital trade, see Mira Burri and Thomas Cottier (eds), *Trade Governance in the Digital Age* (Cambridge: Cambridge University Press, 2012); Mira Burri, 'The International Economic Law Framework for Digital Trade', *Zeitschrift für Schweizerisches Recht* 135 (2015), 10–72.

digital trade and 95 have dedicated electronic commerce chapters.[7] Although the pertinent rules remain highly heterogeneous and differ as to issues covered, the level of commitments and their binding nature, it is overall evident that the trend towards more and more detailed provisions on digital trade has intensified significantly over the years.[8] This regulatory push in the domain of digital trade can be explained with the increased importance of the issue over the years but also with the role played by the United States (US).[9]

The US has over the years endorsed its 'Digital Agenda'[10] through the FTA channel. The agreements reached since 2002 with Australia, Bahrain, Chile, Morocco, Oman, Peru, Singapore, the Central American countries, Panama, Colombia, and South Korea, all contain critical, albeit with different depth of commitment, provisions in the broader field of digital trade. The diffusion of the US template is not however limited to US agreements[11] and has been replicated in a number of other FTAs as well, such as Singapore–Australia, Thailand–Australia, New Zealand–Singapore, Japan–Singapore, and South Korea–Singapore. Many, also smaller states, such as Chile, have become active in the area of data governance; at the same time many other countries, such as those parties to the European Free Trade Area (EFTA),[12] have not yet implemented distinct digital trade strategies.[13] The EU, although to be reckoned with as a major actor in international economic law and policy, has also been a rather late-comer into the digital trade rulemaking domain, as the chapter reveals below.

The relevant aspects of digital trade governance can be found in: (1) the specifically dedicated electronic commerce FTA chapters; (2) the chapters on cross-border supply of services (with particular relevance of the telecommunications, computer and related, audiovisual and financial services sectors); as well as in (3) the IP chapters.[14] This chapter focuses exclusively on the electronic commerce/digital trade chapters, as well

[7] This analysis is based on a dataset of all digital trade relevant norms in trade agreements (TAPED). See Mira Burri and Rodrigo Polanco, 'Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset' *Journal of International Economic Law* 23 (2020), 187–220. For all data, as well as updates of the dataset, see https://unilu.ch/taped

[8] For an overview of the FTA developments, see Mira Burri, 'Data Flows and Global Trade Law', in Mira Burri (ed), *Big Data and Global Trade Law* (Cambridge: Cambridge University Press, 2021), 11–41.

[9] See Manfred Elsig and Sebastian Klotz, 'Data Flow-Related Provisions in Preferential Trade Agreements: Trends and Patterns of Diffusion', in Mira Burri (ed), *Big Data and Global Trade Law* (Cambridge: Cambridge University Press, 2021), 42–62.

[10] US Congress, Bipartisan Trade Promotion Authority Act of 2001, H. R. 3005, 3 October 2001; Sacha Wunsch-Vincent, 'The Digital Trade Agenda of the US', *Aussenwirtschaft* 1 (2003), 7–46; also Henry Gao, 'Regulation of Digital Trade in US Free Trade Agreements: From Trade Regulation to Digital Regulation', *Legal Issues of Economic Integration* 45 (2018), 47–70.

[11] Elsig and Klotz, supra note 9.

[12] The EFTA Members comprise Iceland, Lichtenstein, Norway and Switzerland.

[13] It should be noted in this context that the EFTA countries have now adopted a model electronic commerce chapter but it is yet to be implemented in a treaty text.

[14] For analysis of all relevant chapters, see Mira Burri, 'The Regulation of Data Flows in Trade Agreements', *Georgetown Journal of International Law* 48 (2017), 408–448.

as on the specific digital economy agreements, which have become the new and critical source of new rulemaking in the area of digital trade.

The electronic commerce chapters play a dual role in the landscape of trade rules in the digital era. On the one hand, they represent an attempt to compensate for the lack of progress in the WTO and address many of the questions of the WTO Electronic Commerce Programme that have been discussed but not resolved.[15] For instance, a majority of the chapters recognize the applicability of WTO rules to electronic commerce[16] and establish an express and permanent duty-free moratorium on electronic transmissions.[17] In most of the templates tailored along the US model, the chapters also include a definition of 'digital products', which treats products delivered offline equally as those delivered online,[18] so that technological neutrality is ensured and some of the classification dilemmas under the General Agreement on Trade in Services (GATS) cast aside (in particular when combined with negative committing for services[19]). The electronic commerce chapters increasingly cover also regulatory questions that have not been treated in the WTO context – the so-called 'WTO-extra' issues. One can group these rules into two broader categories: (1) rules that seek to enable digital trade in general, by tackling distinct issues, such as paperless trading and electronic authentication; and (2) rules that address cross-border data, new digital trade barriers and novel issues, which can encompass questions ranging from cybersecurity to open government data. It should be noted that as to the first cluster of issues on the facilitation of digital trade, the number of FTAs that contain such rules is substantial and one can observe convergence, still only few agreements include rules on data.[20]

B. Emerging Templates for Digital Trade and Stakeholder Positioning

In the following sections, the chapter looks at the new rules created in recent agreements through a detailed analysis of the most advanced electronic commerce chapters thus far – those of the CPTPP, the USMCA, and the dedicated digital economy agreements. We complement this analysis with an enquiry into the EU treaties and the EU's repositioning on data flows in particular, and into the RCEP as the first agreement with digital trade provisions to include China. The purpose is two-prong – on the one hand to highlight legal innovation in these treaties and to give a sense of the positions of the major stakeholders, on the other.

---

[15] Sacha Wunsch-Vincent, *The WTO, the Internet and Digital Products: EC and US Perspectives* (Oxford: Hart, 2006).

[16] See e.g. US–Singapore FTA, Article 14.1; US–Australia FTA, Article 16.1.

[17] See e.g. US–Singapore FTA, Article 14.3, para. 1; US–Chile FTA, Article 15.3. For a discussion of the variety of rules on the moratorium, see Burri and Polanco, supra note 7.

[18] See e.g. US–Singapore FTA, Article 14.3; US–Australia FTA, Article 16.4.

[19] See e.g. Burri (2017), supra note 14.

[20] See Burri and Polanco, supra note 7; also Mira Burri, 'The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation' *UC Davies Law Review* 51 (2017), 65–132.

1. The Comprehensive and Progressive Agreement for Transpacific Partnership

The Comprehensive and Progressive Agreement for Transpacific Partnership was agreed upon in 2017 between eleven countries in the Pacific Rim[21] and entered into force on 30 December 2018. Beyond the economic significance of the agreement,[22] the CPTPP chapter on electronic commerce created the most comprehensive template in the landscape of FTAs. It should be noted that despite the US having dropped out of the planned Transpacific Partnership Agreement (TPP) with the start of the Trump administration, the CPTPP chapter reflects the US efforts under its updated 'Digital 2 Dozen' agenda[23] to secure obligations on digital trade[24] and is a verbatim reiteration of the TPP chapter. A closer look at the CPTPP electronic commerce chapter is therefore well-deserved.

In the first part and not unusually for US-led and other FTAs, the CPTPP electronic commerce chapter clarifies that it applies 'to measures adopted or maintained by a Party that affect trade by electronic means'[25] but excludes from this broad scope (1) government procurement and (2) information held or processed by or on behalf of a Party, or measures related to such information, including measures related to its collection.[26] For greater certainty, measures affecting the supply of a service delivered or performed electronically are subject to the obligations contained in the relevant provisions on investment and services;[27] some additional exceptions are also specified.[28] The following provisions address, again as customarily, some of the leftovers of the WTO Electronic Commerce Programme and provide for the facilitation of online commerce. In this sense, Article 14.3 CPTPP bans the imposition of customs duties on electronic transmissions, including content transmitted electronically, and Article 14.4 endorses the non-discriminatory treatment of digital products,[29] which are defined broadly pursuant to Article 14.1.[30] Article 14.5 CPTPP is meant to shape the

---

[21] Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore and Vietnam.

[22] See e.g. Zachary Torrey, 'TPP 2.0: The Deal Without the US: What's New about the CPTPP and What Do the Changes Mean?' *The Diplomat*, 3 February 2018.

[23] See https://ustr.gov/about-us/policy-offices/press-office/reports-and-publications/2016/digital-2-dozen

[24] See also in this sense New Zealand's Waitangi Tribunal, Report on the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (November 2021), at 72 and passim.

[25] Article 14.2(2) CPTPP.

[26] Article 14.2(3) CPTPP. For the lack of guidance and the potential contentions around the scope of this exception, see the different experts' opinions in New Zealand's Waitangi Tribunal, Report on the Comprehensive and Progressive Agreement for Trans-Pacific Partnership, supra note 24, at 81–83.

[27] Article 14.2(4) CPTPP.

[28] Article 14.2(5) and (6) CPTPP.

[29] The obligation does not apply to subsidies or grants, including government-supported loans, guarantees and insurance, nor to broadcasting. It can also be limited through the rights and obligations specified in the IP chapter. Article 14.2(3) CPTPP.

[30] Digital product means a computer programme, text, video, image, sound recording or other product that is digitally encoded, produced for commercial sale or distribution, and that can be transmitted electronically. Two specifications in the footnotes apply: (1) digital product does not include a digitized representation of a financial instrument, including money; and (2) the definition of digital product should

domestic electronic transactions framework by including binding obligations for the parties to follow the principles of the UNCITRAL Model Law on Electronic Commerce 1996 or the UN Convention on the Use of Electronic Communications in International Contracts. Parties must endeavour to (1) avoid any unnecessary regulatory burden on electronic transactions; and (2) facilitate input by interested persons in the development of its legal framework for electronic transactions.[31] The provisions on paperless trading and on electronic authentication and electronic signatures complement this by securing equivalence of electronic and physical forms. With regard to paperless trading, it is clarified that parties shall endeavour to make trade administration documents available to the public in electronic form and accept trade administration documents submitted electronically as the legal equivalent of the paper version.[32] The norm on electronic signatures is more binding and provides that parties shall not deny the legal validity of a signature solely on the basis that the signature is in electronic form,[33] nor shall they adopt or maintain measures that prohibit parties to an electronic transaction from mutually determining the appropriate authentication methods for that transaction; or prevent such parties from having the opportunity to establish before judicial or administrative authorities that their transaction complies with legal requirements with respect to authentication.[34]

The remainder of the provisions found in the CPTPP electronic commerce chapter can be said to belong to the second and more innovative category of rulemaking that tackles the emergent issues of the data-driven economy. Most importantly, the CPTPP explicitly seeks to curb data protectionism. First, it does so through an explicit ban on the use of data localization measures. Article 14.13(2) prohibits the parties from requiring a 'covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory'. Second, the CPTPP replaces the soft language from the US–South Korea FTA on free data flows and frames it as a hard rule: '[e]ach 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'.[35] The rule has a broad scope and most data transferred over the Internet is likely to be covered.

Measures restricting digital flows or implementing localization requirements are permitted only if they do not amount to 'arbitrary or unjustifiable discrimination or a disguised restriction on trade' and do not 'impose restrictions on transfers of

not be understood to reflect a Party's view on whether trade in digital products through electronic transmission should be categorized as trade in services or trade in goods. Article 14(1) includes two footnotes clarifying that: 'For greater certainty, digital product does not include a digitised representation of a financial instrument, including money' (footnote 2) and 'The definition of digital product should not be understood to reflect a Party's view on whether trade in digital products through electronic transmission should be categorised as trade in services or trade in goods' (footnote 3).

[31] Article 14.5(2) CPTPP.

[32] Article 14.9 CPTPP.

[33] Article 14.6(1) CPTPP.

[34] Article 14.6(2) CPTPP.

[35] Article 14.11(2) CPTPP.

information greater than are required to achieve the objective'.[36] These non-discriminatory conditions are similar to the strict test formulated by Article XIV GATS and Article XX GATT 1994 – a test that is supposed to balance trade and non-trade interests by 'excusing' certain violations but that is also extremely hard to pass, as the WTO jurisprudence has thus far revealed.[37] The CPTPP test differs from the WTO norms in two significant elements: (1) while there is a list of public policy objectives in the GATT 1994 and the GATS, the CPTPP provides no such enumeration and simply refers to a 'legitimate public policy objective';[38] (2) in the chapeau-like reiteration of 'arbitrary or unjustifiable discrimination', there is no GATT or GATS-like qualification of 'between countries where like conditions prevail'. The scope of the exception is thus unclear – it can be linked to legal uncertainty, as well as to potentially unworkable safeguards for domestic constituencies.[39] Lastly, it should be noted that the ban on localization measures is softened on financial services and institutions.[40] An annex to the Financial Services chapter has a separate data transfer requirement, whereby certain restrictions on data flows may apply for the protection of privacy or confidentiality of individual records, or for prudential reasons.[41] Government procurement is also excluded.[42]

The CPTPP addresses other novel issues as well – one of them is source code. Pursuant to Article 14.17, a CPTPP Member may not require the transfer of, or access to, source code of software owned by a person of another Party as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory. The prohibition applies only to mass-market software or products containing such software.[43] This means that tailor-made products are excluded, as well as software used for critical infrastructure and those in commercially negotiated contracts.[44] The aim of this provision is to protect software companies and address their concerns about loss of IP or cracks in the security of their proprietary code; it may also

[36] Article 14.11(3) CPTPP.

[37] See e.g. Henrik Andersen, 'Protection of Non-Trade Values in WTO Appellate Body Jurisprudence: Exceptions, Economic Arguments, and Eluding Questions', *Journal of International Economic Law* 18 (2015), 383–405.

[38] Article 14.11(3) CPTPP.

[39] See e.g. in this sense New Zealand's Waitangi Tribunal, Report on the Comprehensive and Progressive Agreement for Trans-Pacific Partnership, supra note 24, in particular at 132–142.

[40] See the definition of 'a covered person' (Article 14.1 CPTPP), which excludes a 'financial institution' and a 'cross-border financial service supplier'.

[41] The provision reads: 'Each Party shall allow a financial institution of another Party to transfer information in electronic or other form, into and out of its territory, for data processing if such processing is required in the institution's ordinary course of business'.

[42] Article 14.8(3) CPTPP.

[43] Article 14.17(2) CPTPP.

[44] Ibid. On the possible interpretations of the provision and difference to including algorithms, see New Zealand's Waitangi Tribunal, Report on the Comprehensive and Progressive Agreement for Trans-Pacific Partnership, supra note 24, at 104–112.

be interpreted as a reaction to China's demands to access to source code from software producers selling in its market.[45]

These provisions illustrate an important development in the FTA rulemaking in that, they do not merely seek the reduction of trade barriers but effectively shape the regulatory space domestically. Particularly critical in this context are also the rules in the area of data protection. Article 14.8(2) requires every CPTPP party to 'adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce'. Yet, there are no standards or benchmarks for the legal framework specified, except for a general requirement that CPTPP parties 'take into account principles or guidelines of relevant international bodies'.[46] A footnote provides some clarification in saying that: '… a Party may comply with the obligation in this paragraph by adopting or maintaining measures such as a comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy'.[47] Parties are also invited to promote compatibility between their data protection regimes, by essentially treating lower standards as equivalent.[48] The goal of these norms can be interpreted as a prioritization of trade over privacy rights. This has been pushed by the US during the TPP negotiations, as the US subscribes to a relatively weak and patchy protection of privacy.[49] Timewise, this push came also at the phase, when the US was wary that it could lose the privilege of transatlantic data transfer, as a consequence of the judgment of the Court of Justice of European Union (CJEU) that struck down the EU–US Safe Harbour Agreement.[50]

Next to these important data protection provisions, the CPTPP also includes norms on consumer protection[51] and spam control,[52] as well as for the first time rules on cybersecurity. Article 14.16 is however non-binding and identifies a limited scope of

[45] See e.g. Joint Statement on Trilateral Meeting of the Trade Ministers of the United States, Japan, and the European Union, Washington, D.C., 14 January 2020, available at: https://trade.ec.europa.eu/doclib/docs/2020/january/tradoc_158567.pdf

[46] Article 14.8(2) CPTPP.

[47] Ibid., at footnote 6.

[48] Article 14.8(5) CPTPP.

[49] See e.g. James Q. Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' *The Yale Law Journal* 113 (2004), 1151–1221; Paul M. Schwartz and Daniel J. Solove, 'Reconciling Personal Information in the United States and European Union', *California Law Review* 102 (2014), 877–916; also Burri (2021), supra note 5.

[50] Case C-362/14 *Schrems*, judgment of 6 October 2015, EU:C:2015:650. Maximillian Schrems is an Austrian citizen, who filed a suit against the Irish supervisory authority, after it rejected his complaint over Facebook's practice of storing user data in the US. The plaintiff claimed that his data was not adequately protected in light of the NSA revelations and this, despite the existing agreement between the EU and the US – the so-called 'safe harbor' scheme. The later EU-US Privacy Shield arrangement has been also rendered invalid by a judgment in 2020: Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems (Schrems II),* judgment of 16 July 2020, ECLI:EU:C:2020:559. A political solution for transatlantic data flows has only been recently found in March 2022 with the legal texts still pending.

[51] Article 14.17 CPTPP.

[52] Article 14.14 CPTPP.

activities for cooperation, in situations of 'malicious intrusions' or 'dissemination of malicious code', and capacity-building of governmental bodies dealing with cybersecurity incidents. Net neutrality is another important digital economy topic that has been given specific attention in the CPTPP, although the so created rules are of non-binding nature.[53] The norm comes with a number of exceptions from the domestic laws of the CPTPP parties and permits deviations from undefined situations that call for 'reasonable network management' or exclusive services.[54] As the obligations are unlinked to remedies for situations, such as blocking, throttling, discriminating or filtering content, it is unlikely that the CPTPP would lead to uniform approach with regard to net neutrality across the CPTPP countries.

The approval for the UK to accede to the CPTPP[55] and recent requests for accession by and China and Taiwan[56] potentially expand the commercial reach and geopolitical dimension of this agreement. Next to these possibilities for an enlarged CPTPP membership, it should also be pointed out that the CPTPP model has diffused in a substantial number of other agreements, such as the 2016 Chile–Uruguay FTA, the 2016 updated Singapore–Australia FTA (SAFTA), the 2017 Argentina–Chile FTA, the 2018 Singapore–Sri Lanka FTA, the 2018 Australia–Peru FTA, the 2019 Brazil–Chile FTA, the 2019 Australia–Indonesia FTA, the 2018 USMCA, the 2019 Japan–US Digital Trade Agreement, as well as in a number of DEAs. The chapter discusses first the USMCA and then looks at selected DEAs.

2. The United States Mexico Canada Agreement

After the withdrawal of the United States from the TPP, there was some uncertainty as to the direction the US will follow in its trade deals in general and on matters of digital trade in particular. The renegotiated NAFTA, which is now referred to as the 'United States Mexico Canada Agreement' (USMCA), provides a useful confirmation of the US approach. The USMCA has a comprehensive electronic commerce chapter, which is now also properly titled 'Digital Trade', follows all critical lines of the CPTPP and creates an even more ambitious template. With regard to replicating the CPTPP model the USMCA follows the same broad scope of application,[57] ban customs duties on electronic transmissions[58] and binds the parties for non-discriminatory treatment of

[53] Article 14.10 CPTPP.

[54] Article 14.10(a) CPTPP. Footnote 6 to this paragraph specifies that: 'The Parties recognise that an Internet access service supplier that offers its subscribers certain content on an exclusive basis would not be acting contrary to this principle'.

[55] On 1 February 2021, the UK formally requested to join the CPTPP and on 2 June 2021, the CPTPP commission agreed to start negotiations. For details on the UK's goals, see UK Department for International Trade*, UK Accession to CPTPP: The UK's Strategic Approach* (London: Department for International Trade, 2021).

[56] US Congressional Research Service, 'China and Taiwan Both Seek to Join the CPTPP', 24 September 2021, at https://crsreports.congress.gov/product/pdf/IN/IN11760

[57] Article 19.2 USMCA.

[58] Article 19.3 USMCA.

digital products.[59] Furthermore, it provides for a domestic regulatory framework that facilitates online trade by enabling electronic contracts,[60] electronic authentication and signatures,[61] and paperless trading.[62]

The USMCA follows the CPTPP model also with regard to data issues and ensures the free flow of data through a clear ban on data localization[63] and a hard rule on free information flows.[64] Article 19.11 specifies further that parties can adopt or maintain a measure inconsistent with the free flow of data provision, if this is necessary to achieve a legitimate public policy objective, provided that there is no arbitrary or unjustifiable discrimination nor a disguised restriction on trade; and the restrictions on transfers of information are not greater than necessary to achieve the objective.[65]

Beyond these similarities, the USMCA introduces some novelties. The first is that the USMCA departs from the standard US approach and signals abiding to some data protection principles and guidelines of relevant international bodies. After recognizing 'the economic and social benefits of protecting the personal information of users of digital trade and the contribution that this makes to enhancing consumer confidence in digital trade,'[66] Article 19.8 USMCA requires from the parties to 'adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade. In the development of its legal framework for the protection of personal information, each Party should take into account principles and guidelines of relevant international bodies, such as the APEC Privacy Framework and the OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013)'.[67] The parties also recognize key principles of data protection, which include: limitation on collection; choice; data quality; purpose specification; use limitation; security safeguards; transparency; individual participation; and accountability,[68] and aim to provide remedies for any violations.[69] This is interesting because it may go beyond what the US has in its national laws on data protection (at least so far[70]) and also because it reflects some of the principles the EU has advocated for in the domain of privacy protection, not only within the boundaries of the Union but also under the Council of Europe. One can of course wonder whether this is a development caused by the so-called 'Brussels effect',

[59] Article 19.4 USMCA.
[60] Article 19.5 USMCA.
[61] Article 19.6 USMCA.
[62] Article 19.9 USMCA.
[63] Article 19.12 USMCA.
[64] Article 19.11 USMCA.
[65] Article 19.11(2) USMCA. There is a footnote attached, which clarifies: A measure does not meet the conditions of this paragraph if it accords different treatment to data transfers solely on the basis that they are cross-border in a manner that modifies the conditions of competition to the detriment of service suppliers of another Party. The footnote does not appear in the CPTPP treaty text.
[66] Article 19.8(1) USMCA.
[67] Article 19.8(2) USMCA.
[68] Article 19.8(3) USMCA.
[69] Article19.8(4) and (5) USMCA.
[70] Chander and Schwarz, supra note 5.

whereby the EU 'exports' its own domestic standards and they become global,[71] or whether we are seeing a shift in US privacy protection regimes as well.[72]

Beyond data protection, three further innovations of the USMCA may be mentioned. The first refers to the inclusion of 'algorithms', the meaning of which is 'a defined sequence of steps, taken to solve a problem or obtain a result'[73] and has become part of the ban on requirements for the transfer or access to source code in Article 19.16.[74] The second novum refers to the recognition of 'interactive computer services' as particularly vital to the growth of digital trade. Parties pledge in this sense not to 'adopt or maintain measures that treat a supplier or user of an interactive computer service as an information content provider in determining liability for harms related to information stored, processed, transmitted, distributed, or made available by the service, except to the extent the supplier or user has, in whole or in part, created, or developed the information'.[75] This provision is important, as it seeks to clarify the liability of intermediaries and delineate it from the liability of host providers with regard to IP rights' infringement. It also secures the application of Section 230 of the US Communications Decency Act,[76] which insulates platforms from liability[77] but has been recently under attack in many jurisdictions in the face of fake news and other negative developments related to platforms' power.[78]

---

[71] Anu Bradford, 'The Brussels Effect', *Northwestern University Law Review* 107 (2012), 1–68; Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford: Oxford University Press, 2020).

[72] See Anupam Chander, Margot E. Kaminski and William McGeveran, 'Catalyzing Privacy Law', *Minnesota Law Review* 105 (2021), 1733–1802.

[73] Article 19.1 USMCA.

[74] On the expansion of the scope of the source code provision, see New Zealand's Waitangi Tribunal, supra note 24, at 104–112.

[75] Article 19.17(2) USMCA. Annex 19-A creates specific rules with the regard to the application of Article 19.17 for Mexico, in essence postponing its implementation for three years. There is also a footnote to the provision, which specifies that a party may comply through 'application of existing legal doctrines as applied through judicial decisions'. For the argument that Canada's policy space has remained intact, see Robert Wolfe, 'Learning about Digital Trade: Privacy and E-Commerce in CETA and TPP', *World Trade Review* 18 (2019), s63–s84, at s78.

[76] Section 230 reads: 'No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider' and in essence protects online intermediaries that host or republish speech.

[77] See e.g. Eric Goldman, 'Why Section 230 Is Better Than the First Amendment', *Notre Dame Law Review Reflection* 95 (2019), 33–46; Eric Goldman, 'An Overview of the United States' Section 230 Internet Immunity', in Giancarlo Frosio (ed), *The Oxford Handbook of Online Intermediary Liability* (Oxford: Oxford University Press, 2020), 155–171; Tanner Bone, 'How Content Moderation May Expose Social Media Companies to Greater Defamation Liability', *Washington University Law Review* 98 (2021), 937–963.

[78] See e.g. Lauren Feine, 'Big Tech's Favorite Law Is under Fire', CNBC, 19 February 2020. For an analysis of the free speech implications of digital platforms and literature review, see Mira Burri, 'Fake News in Times of Pandemic and Beyond: An Enquiry into the Rationales for Regulating Information Platforms', in Klaus Mathis and Avishalom Tor (eds), *Law and Economics of the Coronavirus Crisis* (Berlin: Springer, 2022), 31–58.

The third and rather liberal commitment of the USMCA parties is with regard to open government data. This is truly innovative and very relevant in the domain of domestic regimes for data governance. In Article 19.18, the parties recognize that facilitating public access to and use of government information fosters economic and social development, competitiveness, and innovation. 'To the extent that a Party chooses to make government information, including data, available to the public, it shall endeavour to ensure that the information is in a machine-readable and open format and can be searched, retrieved, used, reused, and redistributed'.[79] There is in addition an endeavour to cooperate, so as to 'expand access to and use of government information, including data, that the Party has made public, with a view to enhancing and generating business opportunities, especially for small and medium-sized enterprises'.[80] Finally, it can be mentioned that the cooperation provision of the USMCA goes beyond the CPTPP[81] and envisages an institutional setting to enable this cooperation, 'or any other matter pertaining to the operation of this chapter'.[82]

The US approach towards digital trade issues has been confirmed by the recent US–Japan DTA, signed on 7 October 2019, alongside the US–Japan Trade Agreement.[83] The US–Japan DTA replicates almost all provisions of the USMCA and the CPTPP,[84] including the rules on open government data,[85] source code[86] and interactive computer services[87] but notably covering also financial and insurance services as part of the scope of agreement. In the current WTO negotiations on electronic commerce, the US has endorsed an ambitious template, which is essentially a compilation of the USMCA and the DTA.[88]

[79] Article 19.18(2) USMCA.

[80] Article 19.8(3) USMCA.

[81] The provision envisages amongst other things linked to enabling global digital trade, exchange of information and experience on personal information protection, particularly with the view to strengthening existing international mechanisms for cooperation in the enforcement of laws protecting privacy; and cooperation on the promotion and development of mechanisms, including the APEC Cross-Border Privacy Rules, that further global interoperability of privacy regimes. See Article 19.14(1) USMCA, at paras. (a)(i) and (b) respectively.

[82] Article 19.14(2) USMCA.

[83] For the text of the agreements, see: https://ustr.gov/countries-regions/japan-korea-apec/japan/us-japan-trade-agreement-negotiations/us-japan-digital-trade-agreement-text

[84] Article 7: Customs Duties; Article 8: Non-Discriminatory Treatment of Digital Products; Article 9: Domestic Electronic Transactions Framework; Article 10: Electronic Authentication and Electronic Signatures; Article 14: Online Consumer Protection; Article 11: Cross-Border Transfer of Information; Article 12: Location of Computing Facilities; Article 16: Unsolicited Commercial Electronic Messages; Article 19: Cybersecurity US–Japan DTA.

[85] Article 20 US–Japan DTA.

[86] Article 17 US–Japan DTA.

[87] Article 18 US–Japan DTA. A side letter recognizes the differences between the US and Japan's systems governing the liability of interactive computer services suppliers and parties agree that Japan need not change its existing legal system to comply with Article 18.

[88] WTO, Joint Statement on Electronic Commerce, Communication from the United States, INF/ECOM/5, 25 March 2019; WTO, Joint Statement on Electronic Commerce, Communication from the United States, INF/ECOM/23, 26 April 2019.

3. Digital Economy Agreements

The increased preoccupation of policymakers with digital trade issues can be perhaps best exemplified by the new generation of the so-called 'digital economy agreements' (DEAs). This is a relatively new phenomenon in the trade rulemaking landscape and so far only six such treaties have been adopted – the aforementioned US–Japan Digital Trade Agreement; the 2019 ASEAN Agreement on Electronic Commerce (within the context of ASEAN); the 2020 Singapore–Australia Digital Economy Agreement (ASDEA); the 2020 Digital Economy Partnership Agreement (DEPA) between Chile, New Zealand, Singapore; the 2021 Korea–Singapore DEA and the 2022 UK–Singapore DEA. What is key to mention at the outset is that these agreements can be adopted as stand-alone initiatives, such as the DEPA, or as part of existing or new trade agreements, such as the ones between Japan and the US, Singapore and Australia, and the UK and Singapore. The DEAs may also differ in scope and the extent to which they include new items on the regulation of the data-driven economy. So, while for instance the US–Japan DTA still very much resembles a conventional, albeit extended, digital trade chapter, the ASDEA, the DEPA, the UK–Singapore DEA go beyond this and engage in entirely new areas of regulatory cooperation, including a mixed set of hard and soft law provisions. This section looks more closely at the DEPA as representative of this latter category and as a model of innovative digital trade rulemaking.

The 2020 DEPA between Chile, New Zealand, and Singapore,[89] all parties also to the CPTPP, is, as earlier noted, not conceptualized as a purely trade agreement but one that is meant to address the broader issues of the digital economy. In this sense, its scope is wide, open and flexible and covers several emergent issues, such as those in the areas of artificial intelligence (AI) and digital inclusion. The agreement is also not a closed deal but one that is open to other countries[90] and the DEPA is meant to complement the WTO negotiations on electronic commerce and build upon the digital economy work underway within APEC, the OECD and other international forums. To enable flexibility and cover a wide range of issues, the DEPA follows a modular approach that provides countries with more options to pick-and-choose and is very different from the 'all-or-nothing' approach of conventional trade treaties.[91] After Module 1, specifying general definitions and initial provisions, Module 2 focuses on 'Business and Trade Facilitation'; Module 3 covers 'Treatment of Digital Products and Related Issues'; Module 4 'Data Issues'; Module 5 'Wider Trust Environment'; Module 6 'Business and Consumer Trust'; Module 7 'Digital Identities'; Module 8 'Emerging Trends and Technologies'; Module 9 'Innovation and the Digital Economy'; Module 10 'Small and Medium Enterprises Cooperation'; and Module 11 'Digital Inclusion'. The rest of the modules deal with the operationalization and implementation of the DEPA and cover common institutions (Module 12); exceptions (Module 13); transparency

[89] For details and the text of the DEPA, see: https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-concluded-but-not-in-force/digital-economy-partnership-agreement/

[90] Article 16.2 DEPA.

[91] James Bacchus, *The Digital Decide: How to Agree on WTO Rules for Digital Trade*, Special Report (Waterloo, ON: Centre for International Governance Innovation, 2021), at 8.

(Module 14); dispute settlement (Module 15); and some final provisions on amendments, entry into force, accession and withdrawal (Module 16).

The type of rules varies across the different modules. On the one hand, all rules of the CPTPP are replicated, some of the USMCA rules, such as the one on open government data[92] (but not source code), and some of the US–Japan DTA provisions, such as the one on ICT goods using cryptography,[93] have been included too. On the other hand, there are many other rules – so far unknown to trade agreements – that try to facilitate the functioning of the digital economy and enhance cooperation on key issues. So, for instance, Module 2 on business and trade facilitation includes next to the standard CPTPP-like norms,[94] additional efforts 'to establish or maintain a seamless, trusted, high-availability and secure interconnection of each Party's single window to facilitate the exchange of data relating to trade administration documents, which may include: (a) sanitary and phytosanitary certificates and (b) import and export data'.[95] Parties have also touched upon other important issues around digital trade facilitation, such as electronic invoicing (Article 2.5); express shipments and clearance times (Article 2.6); logistics (Article 2.4) and electronic payments (Article 2.7). Module 8 on emerging trends and technologies is also particularly interesting to mention, as it highlights a range of key topics that demand attention by policymakers, such as in the areas of fintech and AI. In the latter domain, the parties agree to promote the adoption of ethical and governance frameworks that support the trusted, safe, and responsible use of AI technologies, and in adopting these AI Governance Frameworks parties would seek to follow internationally-recognized principles or guidelines, including explainability, transparency, fairness, and human-centred values.[96] The DEPA parties also recognize the interfaces between the digital economy and government procurement and broader competition policy and agree to actively cooperate on these issues.[97] Along this line of covering broader policy matters in order to create an enabling environment that is also not solely focused on and driven by economic interests, DEPA deals with the importance of a rich and accessible public domain[98] and digital inclusion, which can cover enhancing cultural and people-to-people links, including between Indigenous Peoples, as well as improving access for women, rural populations, and low socio-economic groups.[99]

[92] Article 9.4 DEPA.

[93] Article 3.4 DEPA. The article also provides detailed definitions of cryptography, encryption, and cryptographic algorithm and cipher.

[94] Article 2.2: Paperless Trading; Article 2.3: Domestic Electronic Transactions Framework.

[95] Article 2.2(5) DEPA. 'Single window' is defined as a facility that allows Parties involved in a trade transaction to electronically lodge data and documents with a single-entry point to fulfil all import, export and transit regulatory requirements (Article 2.1 DEPA).

[96] Article 8.2(2) and (3) DEPA.

[97] Articles 8.3 and 8.4 DEPA.

[98] Article 9.2 DEPA.

[99] Article 11.2 DEPA.

Overall, the DEPA is a unique project[100] that covers well the broad range of issues that the digital economy impinges upon and offers a good basis for harmonization and interoperability of domestic frameworks and international cooperation that adequately takes into account the complex challenges of contemporary data governance that has essential trade but also non-trade elements. Its appeal as a form of enhanced, but also flexible, cooperation on issues of the data-driven economy has been confirmed by Canada's[101] and South Korea's[102] interest to join it, as well as by the follow-up similar DEAs, such as the ones between the UK and Singapore and between Australia and Singapore.

4. EU's Approach to Digital Trade

The EU has been a relatively late mover on digital trade issues and for a long time had not developed a distinct strategy. Although EU's FTAs did include provisions on electronic commerce, such as the 2002 agreement with Chile, the language tended to be cautious, with commitments not exceeding GATS levels, and limited to soft cooperation pledges in the services chapter[103] and in the fields of information technology, information society and telecommunications.[104] In more recent agreements, such as the EU–South Korea FTA (signed in 2009), the language is more concrete and binding, imitating some of the US template provisions – for instance, by confirming the applicability of the WTO Agreements to measures affecting electronic commerce and subscribing to a permanent duty-free moratorium on electronic transmissions. Cooperation is also increasingly framed in more concrete terms and includes mutual recognition of electronic signatures certificates, coordination on Internet service providers' liability, consumer protection, and paperless trading.[105] The EU, as particularly insistent on data protection policies, has also sought commitment from its FTA partners to compatibility with the international standards of data protection.[106]

The 2016 EU agreement with Canada – the Comprehensive Economic and Trade Agreement (CETA) – goes a step further. The CETA provisions concern commitments ensuring (a) clarity, transparency and predictability in their domestic regulatory

[100] For a comparison of the DEPA with existing FTAs, see Marta Soprana, 'The Digital Economy Partnership Agreement (DEPA): Assessing the Significance of the New Trade Agreement on the Block', *Trade, Law and Development* 13 (2021), 143–169.

[101] Government of Canada, Global Affairs, Background: Canada's Possible Accession to the Digital Economy Partnership Agreement, 18 March 2021, available at: https://www.international.gc.ca/trade-commerce/consultations/depa-apen/background-information.aspx?lang=eng

[102] 'South Korea Starts Process to Join DEPA', 6 October 2021, available at: https://en.yna.co.kr/view/PYH20211006124000325

[103] Article 102 EU–Chile FTA. The agreement states that '[t]he inclusion of this provision in this Chapter is made without prejudice of the Chilean position on the question of whether or not electronic commerce should be considered as a supply of services'.

[104] Article 37 EU–Chile FTA.

[105] Article 7.49 EU–South Korea FTA.

[106] Article 7.48 EU–South Korea FTA.

frameworks; (b) interoperability, innovation and competition in facilitating electronic commerce; as well as (c) facilitating the use of electronic commerce by small and medium sized enterprises.[107] The EU has succeeded in deepening the privacy commitments and the CETA has a specific norm on trust and confidence in electronic commerce, which obliges the parties to adopt or maintain laws, regulations or administrative measures for the protection of personal information of users engaged in electronic commerce in consideration of international data protection standards.[108] Yet, there are no deep commitments on digital trade; nor there are any rules on data and data flows.[109]

It is only very recently that the EU took up a more modern, CPTPP-comparable, approach towards the regulation of digital trade. Some indications for this turn were given by the 2018 EU–Japan Economic Partnership Agreement (EPA)[110] and the modernization of the trade part of the EU–Mexico Global Agreement, where for the first time data flows were mentioned but still cautiously, as the Parties only committed to 'reassess' within three years of the entry into force of the agreement, the need for actually including provisions on the free flow of data. The new EU approach towards the issue of cross-border data is now fully endorsed in the EU's currently negotiated deals with Australia and Tunisia, and the 2022 agreement with New Zealand. These FTAs' digital trade chapters include norms on the free flow of data and data localization bans. This repositioning and newer commitments are however also linked with high levels of data protection.[111]

The EU wishes to permit data flows only if coupled with the high standards of its General Data Protection Regulation (GDPR)[112] and endorses a distinct model of privacy as a fundamental right. While the EU and its partners seek to permit the flow of data, these commitments are conditioned: first, by a dedicated article on data protection, which clearly states that: 'Each Party recognises that the protection of personal data and privacy is a *fundamental right* and that high standards in this regard contribute to trust in the digital economy and to the development of trade',[113] followed by a paragraph on data sovereignty: 'Each Party may adopt and maintain the safeguards it deems appropriate to ensure the protection of personal data and privacy, including through the adoption and application of rules for the cross-border transfer of personal data. Nothing in this agreement shall affect the protection of personal data and privacy

[107] Article 16.5 CETA.
[108] Article 16.4 CETA.
[109] See e.g. Wolfe, supra note 75.
[110] Article 8.81 EU–Japan EPA.
[111] See European Commission, Horizontal Provisions for Cross-Border Data Flows and for Personal Data Protection in EU Trade and Investment Agreements, February 2018, available at: https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf
[112] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1 [hereinafter GDPR].
[113] See e.g. Article 6(1) draft EU–Australia FTA (emphasis added). The same wording is found in the EU–New Zealand and the draft EU–Tunisia FTA.

afforded by the Parties' respective safeguards'.[114] The EU also wishes to retain the right to see how the implementation of the provisions on data flows impact the conditions of privacy protection, so there is a review possibility within three years of the entry into force of the agreement, and parties remain free to propose to review the list of restrictions at any time.[115] In addition, there is a broad carve-out, in the sense that: '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] The EU thus reserves ample regulatory leeway for its current and future data protection (and other) measures. The exception is also fundamentally different than the objective necessity test under the CPTPP and the USMCA, or that under WTO law, because it is subjective and safeguards the EU's right to regulate.[117]

The new EU approach has been confirmed by the post-Brexit Trade and Cooperation Agreement (TCA) with the United Kingdom,[118] which replicates all the above provisions, except for the explicit mentioning of data protection as a fundamental right – which can be however presumed, since the UK incorporates the European Convention on Human Rights (ECHR) through the Human Rights Act of 1998 into its domestic law.[119] Yet, as the UK seems to be moving away from the EU FTA model as well as from the GDPR standards domestically, this presumption may be somewhat questioned.

Beyond the topic of data flows and its interface with data protection, it should be noted that the rest of the EU digital trade template includes the issues covered by the CPTPP/USMCA model, such as software source code,[120] facilitation of electronic

[114] See e.g. Article 6(2) draft EU–Australia FTA. The same wording is found in the EU–New Zealand and the draft EU–Tunisia FTA.

[115] See e.g. Article 5(2) draft EU–Australia FTA. The same wording is found in the EU–New Zealand and the draft EU–Tunisia FTA.

[116] See e.g. Article 2 draft EU-–Australia FTA. The same wording is found in the EU–New Zealand and the draft EU–Tunisia FTA.

[117] Svetlana Yakovleva, 'Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy' *University of Miami Law Review* 74 (2020), 416–519, at 496.

[118] Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part, OJ L [2020] 444/14.

[119] See e.g. Kristina Irion and Mira Burri, 'Digitaler Handel (Commentary of the Digital Trade Title of the EU-UK Trade and Cooperation Agreement)', in Gesa Kübek et al. (eds) *Handels- und Kooperationsvertrag EU/GB Handbuch* (Baden-Baden: Nomos, 2022), 343–368.

[120] Article 207 TCA. Again with notable safeguards, specified in paras. 2 and 3 of Article 207, including the general exceptions, security exceptions and prudential carve-out in the context of a certification procedure; voluntary transfer of source code on a commercial basis, a requirement by a court or administrative tribunal, or a requirement by a competition authority pursuant to a Party's competition law to prevent or remedy a restriction or a distortion of competition; a requirement by a regulatory body pursuant to a Party's laws or regulations related to the protection of public safety with regard to users online; the protection and enforcement of IP; and government procurement related measures.

commerce,[121] online consumer protection,[122] spam[123] and open government data;[124] not including however a provision on non-discrimination of digital products and excluding audiovisual services from the scope of the application of the digital trade chapter.[125] This TCA template is also the one that the EU has endorsed under the WTO electronic commerce negotiations.[126]

5. The Regional Comprehensive Economic Partnership

An interesting and much anticipated development against the backdrop of the diverging, at least on data flows, EU and US positions has been the recent Regional Comprehensive Economic Partnership (RCEP) signed on 15 November 2020 between the ASEAN Members,[127] China, Japan, South Korea, Australia and New Zealand and in force since 1 January 2022.[128] Chapter 12 of the RCEP includes the relevant electronic commerce rules. In a similar fashion to the CPTPP, it clarifies its application 'to measures adopted or maintained by a Party that affect trade by electronic means' but excludes from this broad scope (1) government procurement and (2) information held or processed by or on behalf of a Party, or measures related to such information, including measures related to its collection. In addition, key provisions on the location of computing facilities and the cross-border transfer of information by electronic means apply in conformity with obligations established in the chapters on trade in services (Chapter 8) and on investment (Chapter 10). The RCEP electronic commerce chapter rules are grouped into four areas: (1) trade facilitation; (2) creation of a conducive environment for electronic commerce; (3) promotion of cross-border electronic commerce; and (4) others.

With regard to trade facilitation, RCEP includes provisions on paperless trading,[129] on electronic authentication and electronic signatures.[130] On paperless trading, the RCEP Members avoid entering into binding commitments. They, instead, commit to 'works toward', 'endevour', or 'cooperate'.[131] The norms on accepting the validity of

[121] Articles 205 and 206 TCA.
[122] Article 208 TCA.
[123] Article 209 TCA.
[124] Article 210 TCA.
[125] Article 197(2) TCA.
[126] WTO, Joint Statement on Electronic Commerce, EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce, Communication from the European Union, INF/ECOM/22, 26 April 2019; WTO, Joint Statement on Electronic Commerce, Communication from the European Union, INF/ECOM/13, 25 March 2019.
[127] Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam.
[128] RCEP entered into force on 1 January 2022 for ten original parties: Australia, New Zealand, Brunei Darussalam, Cambodia, China, Japan, Laos, Singapore, Thailand and Vietnam. RCEP entered into force for the Republic of Korea on 1 February 2022 and for Malaysia on 18 March 2022. For the details and the text of RCEP, see https://rcepsec.org/legal-text/
[129] Article 12.5 RCEP.
[130] Article 12.6 RCEP.
[131] Article 12.5 RCEP.

electronic signatures are more binding but in contrast to the CPTPP and USMCA, permit for domestic laws and regulations to provide otherwise and prevail in case of inconsistency. Regarding commitments to create a conductive environment for electronic commerce, the inclusion of provisions on online personal information protection[132] and cybersecurity[133] is remarkable. On the former, RCEP Members establish that they shall adopt or maintain a legal framework, which ensures the protection of personal information. Unsurprisingly, RCEP is not prescriptive as to how parties may comply with this obligation. As for the latter aspect on cybersecurity, the parties do not establish a binding provision but recognize the importance of building capabilities and using existing collaboration mechanisms to cooperate. The RCEP Members also commit to adopt or maintain laws or regulations regarding online consumer protection,[134] unsolicited commercial electronic messages,[135] and a framework governing electronic transactions that takes into account international instruments,[136] as well as commit to transparency.[137]

The next grouping of RCEP provisions is critical, as it deals with cross-border data flows. In essence and actually similarly to the EU, the RCEP provides only for conditional data flows, while preserving room for domestic policies, which well may be of data protectionist nature. So, while the RCEP electronic commerce chapter includes a ban on localization measures,[138] as well as a commitment to free data flows,[139] there are clarifications that give RCEP Members a lot of policy space and essentially undermine the impact of the made commitments. In this line, there is an exception possible for legitimate public policies and a footnote to Article 12.14.3(a), which says that: 'For the purposes of this subparagraph, the Parties affirm that the *necessity* behind the implementation of such legitimate public policy *shall be decided* by the implementing Party'. This essentially goes against any exceptions assessment, as we know it under WTO law, and triggers a self-judging mechanism. In addition, subparagraph (b) of Article 12.14.3 says that the provision does not prevent a party from taking 'any measure that it considers necessary for the protection of its *essential security interests*. Such measures shall not be disputed by other Parties'.[140] Article 12.15 on cross-border transfer of information follows the same language and thus secures plenty of policy space, for countries like China or Vietnam, to control data flows without further justification.

[132] Article 12.8 RCEP.
[133] Article 12.13 RCEP.
[134] Article 12.7 RCEP.
[135] Article 12.9 RCEP.
[136] Article 12.10 RCEP.
[137] Article 12.12 RCEP.
[138] Article 12.14 RCEP.
[139] Article 12.15 RCEP.
[140] Emphasis added. The 'essential security interest' language has been endorsed by China also in the framework of the WTO electronic commerce negotiations.

Other provisions contained in the RCEP electronic commerce chapter include the establishment of a dialogue on electronic commerce[141] and a provision on dispute settlement,[142] which is separate from the general RCEP's dispute settlement.[143] Noteworthy are also some things missing from the RCEP: in comparison to the CPTPP, RCEP does not include provisions on custom duties, non-discriminatory treatment of digital products, source code, principles on access to and use of the Internet for electronic commerce and Internet interconnection charge sharing. It is finally interesting to observe that the RCEP does not necessarily reflect China's position in the WTO negotiations, where China has been more cautious and somewhat fuzzy in its demands – for instance, by subscribing to a very narrow definition of digital trade arguing that the negotiations should focus on the discussion of cross-border trade *in goods* enabled by the Internet, together with relevant payment and logistics services, while paying attention to the digitization trend of trade in services,[144] and not engaging in commitments on data flows. It is also interesting to contemplate how China's wish to join the CPTPP would impact on the WTO negotiations as well as largely on the landscape of digital trade rulemaking – perhaps tilting it towards national security and other carve-outs that seriously diminish the value of the made commitments and prejudice legal certainty.

III. Concluding Remarks and Outlook

The above analysis of the developments in FTAs reveals the critical importance of digital trade as a negotiation topic and the substantial efforts made, in particular in recent years, to address it and create an adequate rule-framework. The achievements made in some FTAs and the dedicated digital economy agreements are quite impressive and there is a strand of legal innovation that seeks to tackle not only the 'old' issues raised under the 1998 WTO Electronic Commerce Programme but also the contemporary issues in the context of a global data-driven economy. The regulatory environment is however still highly fluid. Despite convergence on certain issues of digital trade facilitation, there are many points of divergence among the major stakeholders, in particular with regard to permitting cross-border data flows and the interface between economic and non-economic issues, as the latter effectively determine the digital sovereignty of states and their ability to protect the interests of their citizenry. One can also observe two important trends in this context: for one, it is clear that the FTA efforts serve as regulatory laboratories and while reflecting the positions of the key stakeholders do matter for the multilateral endeavours and for what the shape and substance of any agreement on electronic commerce under the umbrella

[141] Article 12.16 RCEP.
[142] Article 12.17 RCEP.
[143] Chapter 12 RCEP. There is a possibility for this to change after a review of the chapter (Article 12.17(3) RCEP).
[144] WTO, Joint Statement on Electronic Commerce, Communication from China, INF/ECOM/19, 24 April 2019, at section 3 (China Communication 1), at para. 2.5.

of the WTO will be.[145] The second trend has to do with the forming of geopolitical blocks with overlaps that may lead to potential contestations, as well as uncertainties as to the impact of the agreements on the ground – in this context, we see for instance that New Zealand is a member of the CPTPP, the RCEP, the DEPA and also has an agreement with the EU; similarly the UK has a deal with the EU, while also entering into ambitious digital trade commitments under DEAs and the CPTPP.

Overall, the regulatory landscape of digital trade rulemaking is likely to remain dynamic, as technological advances would demand new regulatory responses (for instance with regard to AI) and as countries continue to position themselves, either by starting to actively participate in new rulemaking (like many Central and Latin American countries), forming new geo-blocks or by becoming legal entrepreneurs in departure from older stances (like the United Kingdom does in its new generation of FTAs moving away from EU positions). The next years will also test the willingness for international cooperation in the domain of digital trade regulation and to what extent achievements made in the FTA venues can be multilateralized and brought back to the forum of the WTO.[146]

[145] Mira Burri, 'A WTO Agreement on Electronic Commerce: An Enquiry into its Substance and Viability', *Trade Law 4.0 Working Paper* No 1/2021, forthcoming in *Georgetown Journal of International Law* 53 (2023).
[146] Burri, ibid.