

Creating Data Flow Rules through Preferential Trade Agreements

Mira Burri

I. Introduction

The critical importance of data for all economic sectors seems nowadays almost uncontested. Beyond the somewhat flawed mantra of data being the “new oil,”¹ many studies point to the vast potential of data as an enabler of more efficient business operations, highly innovative solutions, and better policy choices in all areas of societal life.² It is noteworthy that this transformative capacity refers not only to “digital native” areas, such as search or social networking, but also to “brick-and-mortar,” physical businesses, such as those in manufacturing or logistics.³ The COVID-19 pandemic has further augmented the value of digital transactions and the significance of data-driven platforms.⁴ Emerging technologies, like Artificial Intelligence (AI), which are thought to be in many senses a game changer,⁵ are also highly dependent on data inputs.⁶ Therefore, solutions in the domain of data governance can in many aspects condition the future of the data-driven economy.

¹ *The World’s Most Valuable Resource Is No Longer Oil, But Data*, ECONOMIST (May 6, 2017), <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>.

² See, e.g., James Manyika et al., *Big Data: The Next Frontier for Innovation, Competition, and Productivity*, MCKINSEY & CO. (May 1, 2011), <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/big-data-the-next-frontier-for-innovation>; VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, *BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK* (2013).

³ Manyika et al., *supra* note 2.

⁴ See, e.g., *E-Commerce, Trade and the Covid-19 Pandemic: Information Note*, WORLD TRADE ORG. (May 4, 2020), https://www.wto.org/english/tratop_e/covid19_e/e-commerce_report_e.pdf.

⁵ See, e.g., Jacques Bughin et al., *Notes from the AI Frontier: Modeling The Impact of AI on the World Economy*, MCKINSEY & CO. (Sept. 4, 2018), <https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-modeling-the-impact-of-ai-on-the-world-economy>.

⁶ KRISTINA IRION & JOSEPHINE WILLIAMS, *PROSPECTIVE POLICY STUDY ON ARTIFICIAL INTELLIGENCE AND EU TRADE POLICY* (2019), <https://www.uva.nl/binaries/content/assets/uva/>

At the same time, as it has been well documented, the increased dependence on data has brought about a set of new concerns. The impact of data collection and use upon privacy has been particularly widely acknowledged by scholars and policymakers, as well as felt by users of digital products and services in everyday life. Such risks have been augmented in the era of Big Data,⁷ which presents certain distinct challenges to the protection of personal data and by extension to the protection of privacy.⁸ Governments have responded to these concerns in a variety of ways. In terms of external safeguards, states have sought new ways to assert control over data—in particular by prescribing diverse measures that “localize” the data, its storage or suppliers, so as to keep it within the state’s sovereign space.⁹ This kind of erecting barriers to data flows, however, does affect trade and may endanger the realization of an innovative data economy,¹⁰ even in a domestic context.¹¹ In terms of internal safeguards, the preoccupation of the perceived perils of Big Data has triggered the reform of data protection laws around the world, perhaps best exemplified by the efforts of the European Union (EU) to set particularly high standards of protection through the adoption of the 2016 General Data Protection Regulation (GDPR).¹² The reform initiatives are, however, not coherent, as they reflect societies’ understandings of constitutional values, relationships between citizens and the state, and the role of the

en/press-office/ivir_artificial-intelligence-and-eu-trade-policy.pdf; Anupam Chander, *Artificial Intelligence and Trade*, in *BIG DATA AND GLOBAL TRADE LAW* 115 (Mira Burri ed., 2021).

⁷ For an introduction on Big Data applications and review of the relevant literature, see Mira Burri, *Understanding the Implications of Big Data and Big Data Analytics for Competition Law: An Attempt for a Primer*, in *NEW DEVELOPMENTS IN COMPETITION BEHAVIOURAL LAW AND ECONOMICS* 241 (Klaus Mathis & Avishalom Tor eds., 2019).

⁸ See, e.g., Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 *NW. J. TECH. & INTELL. PROP.* 239 (2013); Urs Gasser, *Recoding Privacy Law: Reflections on the Future Relationship among Law, Technology, and Privacy*, 130 *HARV. L. REV.* 61 (2016); Sheri B. Pan, *Get to Know Me: Protecting Privacy and Autonomy under Big Data’s Penetrating Gaze*, 30 *HARV. J.L. & TECH.* 239 (2016).

⁹ See Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 *EMORY L.J.* 677 (2015).

¹⁰ Digital Trade in the US and Global Economies, Part 1, Inv. No. 332–531, USITC Pub. 4415 (July 2013); Digital Trade in the US and Global Economies, Part 2, Inv. No. 332–540, USITC Pub. 4485 (Aug. 2014).

¹¹ See, e.g., Martina F. Ferracane, *The Costs of Data Protectionism*, in *BIG DATA AND GLOBAL TRADE LAW* 63 (Mira Burri ed., 2021); Richard D. Taylor, “Data Localization”: *The Internet in the Balance*, 44 *TELECOMM. POL’Y* 102003 (2020).

¹² Regulation (EU) 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), 2016 O.J. (L 119) 1 [hereinafter GDPR].

market, to name but a few.¹³ The striking divergences, both in the perceptions and the regulation of privacy protection across nations, and the fundamental differences between the human rights approach of the EU and the more market-based, non-interventionist approach of the United States,¹⁴ have also meant that conventional forms of international cooperation and an agreement on shared standards of data protection have become highly unlikely.¹⁵

Against this backdrop of a complex and contentious regulatory environment, data and cross-border data flows, in particular, have become one of the relatively new topics in global trade law discussions. With the stalemate at the multilateral forum of the World Trade Organization (WTO)¹⁶ and despite the current reinvigorated e-commerce negotiations,¹⁷ new rule-making has occurred predominantly in preferential trade venues.¹⁸ This chapter aims to shed light on the rules created in preferential trade agreements (PTAs), their evolution over time, and the positioning of the main stakeholders—the EU and the United States. The mapping of the new data governance regime in trade agreements, however, should not be contained to these major players. Therefore, the chapter also seeks to provide a more comprehensive mapping of data-related norms, found in other agreements, to help better understand the big picture of the regulatory framework for digital trade, as well as to highlight trends in rule diffusion and their potential implications.¹⁹

¹³ See, e.g., Anupam Chander et al., *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733 (2021); Fernanda G. Nicola & Oreste Pollicino, *The Balkanization of Data Privacy Regulation*, 123 W. VA. L. REV. 61 (2020); Mira Burri, *Interfacing Privacy and Trade*, 53 CASE W. RES. J. INT'L L. 35 (2021); Anupam Chander & Paul M. Schwartz, *Privacy and/or Trade*, 90 U. CHI. L. REV. 49 (2023).

¹⁴ See, e.g., James Q. Whitman, *The Two Western Cultures of Privacy: Dignity versus Liberty*, 113 YALE L.J. 1151 (2004); Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CALIF. L. REV. 877 (2014); Chander & Schwartz, *supra* note 14.

¹⁵ See, e.g., Nicola & Pollicino, *supra* note 13.

¹⁶ For details, see, e.g., Mira Burri, *The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation*, 51 U.C. DAVIS L. REV. 65 (2017) [hereinafter Burri, *The Governance of Data and Data Flows in Trade Agreements*]; Mira Burri, *The International Economic Law Framework for Digital Trade*, 135 ZEITSCHRIFT FÜR SCHWEIZERISCHES RECHT 10 (2015).

¹⁷ World Trade Org., *Joint Statement on Electronic Commerce*, WTO Doc. WT/L/1056 (Jan. 25, 2019). For details, see Mira Burri, *Towards a New Treaty on Digital Trade*, 55 J. WORLD TRADE 71 (2021); Mira Burri, *A WTO Agreement on Electronic Commerce: An Enquiry into its Legal Substance and Viability*, 53 GEO. WASH. INT'L L. REV. 565 (2023).

¹⁸ Burri, *The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation*, *supra* note 16; Burri, *The International Economic Law Framework for Digital Trade*, *supra* note 16; WORLD TRADE ORG., *WORLD TRADE REPORT 2018: THE FUTURE OF WORLD TRADE: HOW DIGITAL TECHNOLOGIES ARE TRANSFORMING GLOBAL COMMERCE* (2018), https://www.wto.org/english/res_e/publications_e/world_trade_report18_e.pdf.

¹⁹ The information stems from our own dataset *TAPED: Trade Agreement Provisions on Electronic Commerce and Data*. The *TAPED* dataset is available to all to use and further develop under the creative commons (attribution, non-commercial, share-alike) license at the University of Lucerne website (<https://www.unilu.ch/taped>). See Mira Burri & Rodrigo Polanco, *Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset*, 23 J. INT'L ECON. L. 187 (2020).

II. Digital Trade Provisions in PTAs

A. Developments over Time

From the 384 PTAs agreed upon between 2000 and 2022, more than half of the PTAs have provisions related to digital trade. The largest number of provisions is found in e-commerce and intellectual property (IP) chapters; overall, the provisions remain however highly heterogeneous, addressing an array of different issues ranging from customs duties and paperless trading to personal data protection and cybersecurity. The depth of the commitments and the extent of their binding nature can also vary significantly. Tracing the digital trade provisions along a chronological line, it is evident that the inclusion of provisions in PTAs referring explicitly to electronic commerce started early on (with the 2000 Free Trade Agreement (FTA) between Jordan and the United States²⁰) but recent years mark a significant increase of rule-making in the area of digital trade. As of September 2021, specific provisions applicable to e-commerce can be found in 167 PTAs, mostly in dedicated chapters (109). Among the PTAs with digital trade provisions, it is evident that the number of provisions and the level of their detail have also increased significantly over the years. Meanwhile, the United States–Mexico–Canada Agreement (USMCA) with its “Digital Trade” chapter is the most comprehensive with 19 articles comprising 3,206 words. The newer dedicated digital trade agreements go well beyond—the U.S.–Japan Digital Trade Agreement (DTA) has 22 articles and 5,346 words; and the Digital Economy Partnership Agreement (DEPA) between Chile, Singapore, and New Zealand contains 65 articles and 10,887 words.

B. Overview of Data-Related Rules in PTAs

Beyond the unsettled debate on defining “digital trade,”²¹ one can speak of the relevance of trade rules for data and data flows for at least three

²⁰ US-Jordan FTA, art. 7. Almost at the same time, New Zealand and Singapore agreed upon the Closer Economic Partnership Agreement (CEPA), including an article on paperless trading. Two years later, the Australia-Singapore FTA (SAFTA), concluded on February 17, 2003, was the first PTA to have a dedicated chapter on e-commerce.

²¹ See, e.g., WORLD TRADE ORG., *supra* note 18. See also Mira Burri & Anupam Chander, *What Are Digital Trade and Digital Trade Law?*, 117 AJIL UNBOUND 99 (2023), <https://doi:10.1017/aju.2023.14>.

Table 11.1. Overview of Data-Related Provisions in FTAs (2000–2022)*

	Provisions on data flows in e-commerce chapters and DEAs	Provisions on data localization
Soft commitments	23	2
Hard commitments	22	33
Total	45	35

*For all data, see the TAPED dataset at <https://www.unilu.ch/taped>. For details, see Mira Burri, *Data Flows and Global Trade Law*, in *BIG DATA AND GLOBAL TRADE LAW 11* (Mira Burri ed., 2021).

reasons—because (1) they condition the cross-border flow of data by regulating trade in goods and services as well as the protection of intellectual property; (2) they may install certain beyond the border rules that demand changes in domestic regulation—for example, with regard to procedures with electronic signatures or data protection; and (3) trade law can limit the policy space that regulators have at home—that is, calibrate their data sovereignty.²² In addition to this generic framework, whose rules are found both in WTO law and in the WTO-plus preferential treaties, the last decade has witnessed the emergence of entirely new rules that explicitly regulate data flows. Specific data-related provisions²³ are a relatively new phenomenon and can be found primarily in dedicated e-commerce chapters and only in a handful of agreements (see Table 11.1). The rules refer to both the free cross-border flow of data and to banning or limiting data localization requirements. The next sections focus on these provisions, as well as look at the norms regarding data protection, which may condition the free data flow commitments.

1. Rules on Data Flows

It is fair to note at the outset that thus far no common definition of data flows exists, despite the widespread rhetoric around the term and its frequent use in reports and studies.²⁴ Nonetheless, although there are variations in treaty language, there seems to be a tendency for a broad definition of data flows

²² See in this sense Mira Burri, *The Regulation of Data Flows in Trade Agreements*, 48 *GEO. J. INT'L L.* 408 (2017); Francesca Casalini & Javier López González, *Trade and Cross-Border Data Flows* (OECD, Trade Policy Papers No. 220, 2019).

²³ Provisions on the cross-border flow of data can, however, be also found in chapters, dealing with discrete services sectors, where data flows are inherent to the very definition of those services—this is particularly valid for the telecommunications and the financial services sectors.

²⁴ See Casalini & González, *supra* note 22.

(1) where there are bits of information (data) as part of the provision of a service or a product and (2) where this data crosses borders, although the data flows do not neatly coincide with one commercial transaction and the provision of certain service may relate to multiple flows of data.²⁵ So far, there also has not been a distinction between different types of data—for instance, between personal and non-personal data, personal or company data or machine-to-machine data.²⁶ However, personal information is commonly included explicitly in the data-related provisions in PTAs,²⁷ which may lead to clashes with domestic data protection regimes.

If one looks at the evolution of data flow provisions in PTAs, there has been a major transformation in treaty language over the years. Non-binding provisions on data flows appeared quite early. Already in the 2000 Jordan–US FTA, the Joint Statement on Electronic Commerce highlighted the “need to continue the free flow of information,” although no explicit provision in this regard was included. The first agreement having such a provision is the 2006 Taiwan–Nicaragua FTA, where as part of the cooperation activities, the Parties affirmed the importance of working “to maintain cross-border flows of information as an essential element to promote a dynamic environment for electronic commerce.”²⁸ A stronger commitment can be found in the 2007 South Korea–U.S. FTA, where the Parties stated that they “*shall endeavor* to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders.”²⁹

²⁵ Casalini & González, *id.* As the OECD further clarifies: ‘the actual flow of data reflects individual firm choices: accessing the OECD library from Paris, for instance, actually means contacting a server in the United States (the OECD uses a U.S.-based company for its web services). *Id.* at 1. Moreover, with the cloud, data can live in many places at once, with files and copies residing in servers around the world.’

²⁶ For instance, Sen classifies data into personal data referring to data related to individuals; company data referring to data flowing between corporations; business data referring to digitized content such as software and audiovisual content; and social data referring to behavioural patterns determined using personal data, see Nivedita Sen, *Understanding the Role of the WTO in International Data Flows: Taking the Liberalization or the Regulatory Autonomy Path?*, 21 J. INT’L ECON. L. 323, 343–46 (2018). Aaronson and Leblond categorize data into personal data, public data, confidential business data, machine-to-machine data and metadata, although they do not specifically define each of these terms. See Susan Ariel Aaronson & Patrick Leblond, *Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO*, 21 J. INT’L ECON. L. 245 (2018). The OECD has also tried to break the data into different categories. See OECD, DATA IN THE DIGITAL AGE (Mar. 2019), <https://www.oecd.org/going-digital/data-in-the-digital-age.pdf>.

²⁷ It is typically defined as “any information, including data, about an identified or identifiable natural person.” See, e.g., USMCA, art. 19.1.

²⁸ Nicaragua–Taiwan FTA, art. 14.05(c). A similar wording is used in the 2008 Canada–Peru FTA, 2010 Hong Kong–New Zealand FTA, 2011 Korea–Peru FTA, 2011 Central America–Mexico FTA, 2013 Colombia–Costa Rica FTA, 2013 Canada–Honduras FTA, 2014 Canada–Korea FTA, and the 2015 Japan–Mongolia FTA.

²⁹ Korea–US FTA, art. 15.8 (emphasis added).

The first agreement having a binding provision on cross-border information flows is the 2014 Mexico–Panama FTA.³⁰ A much more detailed provision in this regard is found in the 2015 amended version of the Pacific Alliance Additional Protocol (PAAP),³¹ which was modeled along the negotiated text of the 2016 Trans-Pacific Partnership Agreement (TPP). The TPP text has since then influenced all subsequent agreements having data flows provisions, such as notably the CPTPP and the USMCA³²—both endorsing a strong protection of the free flow of data, as discussed in more detail below.

2. Data Localization

Recent PTAs have also started to include provisions on data localization, by either banning or limiting requirements of data localization or data use. An important difference with the data flows provisions is that almost all such provisions are binding.³³ The first agreement with a ban on data localization is the 2015 Japan–Mongolia FTA.³⁴ Later the same year, the 2015 amended PAAP, and as strongly influenced by the parallel TPP negotiations, included a similar provision on the use and location of computer facilities.³⁵ In 2016, the TPP included a clear ban on localization, which was then replicated in the CPTPP and the USMCA. The diffusion of these norms is clearly discernible also in subsequent PTAs: among others, the 2016 Chile–Uruguay FTA³⁶ and the 2016 Updated SAFTA,³⁷ which closely follow the CPTPP template.³⁸

³⁰ Mexico–Panama FTA, art. 14.10 states that each Party ‘shall allow its persons and the persons of the other Party to transmit electronic information, from and to its territory, when required by said person, in accordance with the applicable legislation on the protection of personal data and taking into consideration international practices.’

³¹ PAAP, art. 13.11 (2015).

³² Such as the 2016 Chile–Uruguay FTA (art. 8.10), the 2016 Updated Singapore–Australia Free Trade Agreement (Chapter 14, art. 13), the 2017 Argentina–Chile FTA (art. 11.6), the 2018 Singapore–Sri Lanka FTA (art. 9.9), the 2018 Australia–Peru FTA (art. 13.11), the 2018 Brazil–Chile FTA (art. 10.12) and the 2019 Australia–Indonesia FTA (art. 13.11).

³³ See Table 11.1. One of the few provisions on data localization that are not directly binding is found in the 2017 Argentina–Chile FTA, where the Parties merely recognize the importance of not requiring a person of the other Party to use or locate the computer facilities in the territory of that Party, as a condition for conducting business in that territory and pledge to exchange good practices and current regulatory frameworks regarding servers’ location. See Argentina–Chile FTA, art. 11.7.

³⁴ Article 9.10 Japan–Mongolia FTA stipulates that neither Party shall require a service supplier of the other Party, an investor of the other Party, or an investment of an investor of the other Party in the area of the former Party, to use or locate computing facilities in that area as a condition for conducting its business.

³⁵ PAAP, art. 13.11 *bis* (2015).

³⁶ Chile–Uruguay FTA, art. 8.11.

³⁷ SAFTA, ch. 14, art. 15.

³⁸ Some variations can be found in the 2019 Australia–Indonesia FTA, where a Party may promptly renew a measure in existence at the date of entry into force of the Agreement or amend such a measure to make it less trade restrictive, at any time (art. 13.12(2)). Additionally, the Australia–Indonesia FTA

Table 11.2. Overview of Privacy-Related provisions in PTAs

Total number of provisions	120
Soft commitments	94
Hard commitments	26

3. Privacy and Data Protection

So far, 120 PTAs include binding and non-binding provisions on “data protection” (see Table 11.2). Yet, the way data is protected varies considerably due to the very different positions of the major actors and the inherent tensions between the regulatory goals of data innovation and data protection.³⁹

Earlier agreements dealing with privacy issues consist of non-binding declarations. The 2000 Jordan–US FTA Joint Statement on Electronic Commerce, for instance, merely declares it necessary to ensure the effective protection of privacy regarding to the process of personal data on global information networks; yet it also states that the means for privacy protection should be flexible and Parties should encourage the private sector to develop and implement enforcement mechanisms, such as guidelines and verification and recourse methodologies, recommending the OECD Privacy Guidelines as an appropriate basis for policy development.⁴⁰ Similarly, the 2001 Canada–Costa Rica FTA includes a provision on privacy as part of the Joint Statement on Global Electronic Commerce, with both Parties agreeing to share information on the functioning of their respective data protection regimes.⁴¹ Later agreements include cooperation activities on enhancing the security of personal data in order to improve the level of protection of

stipulates that nothing in the agreement shall prevent a Party from adopting or maintaining any measure that it considers necessary for the protection of its essential security interests (art. 13.12(3) (b)). A second variation is found in the 2018 Singapore–Sri Lanka FTA, the 2018 Australia–Peru FTA and the 2018 Brazil–Chile FTA, which slightly deviate from the CPTPP, as there is no least restrictive measure requirement mentioned. See Singapore–Sri Lanka FTA, art. 9.10; Australia–Peru FTA, art. 13.12; Brazil–Chile FTA, art. 10.13.

³⁹ See, e.g., Whitman, *supra* note 14; Schwartz & Solove, *supra* note 14; Chander & Schwartz, *supra* note 14; Burri, *supra* note 13.

⁴⁰ U.S.–Jordan Joint Statement on Electronic Commerce, June 7, 2000, art. II, <http://www.sice.oas.org/Trade/us-jrd/St.Ecomm.pdf>.

⁴¹ Canada–Costa Rica Joint Statement on Global Electronic Commerce, Mar. 1, 2021, <http://www.sice.oas.org/trade/canrcr/English/e-comme.asp>.

privacy in electronic communications and avoid obstacles to trade that requires transfer of personal data.⁴²

PTAs now increasingly deal with personal data protection with reference to the adoption of domestic standards. While some merely recognize the importance or the benefits of protecting personal information online,⁴³ in several treaties parties specifically commit to adopt or maintain legislation or regulations that protect the personal data or privacy of users,⁴⁴ in relation to the processing and dissemination of data,⁴⁵ which may also include administrative measures,⁴⁶ or the adoption of nondiscriminatory practices.⁴⁷ Few agreements include qualifications of this commitment, in the sense that each Party shall take measures it deems appropriate and necessary considering the differences in existing systems for personal data protection,⁴⁸ that such measures shall be developed insofar as possible,⁴⁹ or that the Parties have the right to define or regulate their own levels of protection of personal data in pursuit or furtherance of public policy objectives, and shall not be required to disclose confidential or sensitive information.⁵⁰ Some PTAs add that in the development of online personal data protection standards, each Party shall

⁴² These activities include sharing information and experiences on regulations, laws and programs on data protection or the overall domestic regime for the protection of personal information; technical assistance in the form of exchange of information and experts; research and training activities; the establishment of joint programs and projects; maintaining a dialogue; holding consultations on matters of data protection; or in general, other cooperation mechanisms to ensure the protection of personal data.

⁴³ Australia-Indonesia FTA, art. 13.7(1); Brazil-Chile FTA, arts. 10.2(5)(f), 10.8.1; EU-Japan EPA, art. 8.78(3); Central America-Korea FTA, art. 14.5(1); Canada-Honduras FTA, art. 16.2(2)(e).

⁴⁴ Australia-Indonesia FTA, art. 13.7(2); Brazil-Chile FTA, art. 10.8.2; USMCA, art. 19.8(1)-(2); Australia-Peru FTA, art. 13.8(1)-(2); Singapore-Sri Lanka FTA, art. 9.7(1)-(2); Argentina-Chile FTA, art. 11.5(1)-(2); CETA, art. 16.4; Australia-Singapore FTA, Ch. 14, art. 9.1-2 (2016); Chile-Uruguay FTA, art. 8.7(1)-(2); CPTPP, art. 14.8(1)-(2); Singapore-Turkey FTA, art. 9.7(1)-(2); China-Korea FTA, art. 13.5; EAEU-Vietnam FTA, art. 13.5; Korea-Vietnam FTA, art. 10.6(1); Japan-Mongolia FTA, art. 9.6(3); Australia-Japan FTA, art. 13.8(1); Australia-Korea FTA, art. 15.8; Mexico-Panama FTA, art. 14.8; PAAP, art. 13.8(1); Colombia-Panama FTA, art. 19.6; New Zealand-Taiwan FTA, ch. 9, art. 2(d)(i); Colombia-Korea FTA, art. 12.3; Chile-China FTA, art. 55 (2018); Australia-Malaysia FTA, art. 15.8(1); Canada-Colombia FTA, art. 1506.1.

⁴⁵ Central America-EFTA, annex II, art. 1(c)(i); EFTA-GCC FTA, annex XVI, article 1(c)(i); EFTA-Colombia FTA, annex I, art. 1(c)(i); EFTA-Peru FTA, annex I, art. 1(c)(i).

⁴⁶ Colombia-Costa Rica FTA, art. 16.6(1); Korea-Peru FTA, art. 14.7; Hong Kong-New Zealand FTA, ch. 10, art. 2.1(f); ASEAN-Australia-New Zealand FTA, ch. 10, art. 7.1-2; Australia-Chile FTA, art. 16.8; Canada-Peru FTA, art. 1507.

⁴⁷ Australia-Indonesia FTA, art. 13.6(3); Brazil-Chile FTA, art. 10.8(3); USMCA, art. 19.8(4); Australia-Peru FTA, art. 13.8(3); Australia-Chile FTA, art. 11.5(3); Australia-Singapore FTA, ch. 14, art. 9.3 (2016); CPTPP, art. 14.8(3).

⁴⁸ Australia-China FTA, art. 12.8(1); Chile-Thailand FTA, art. 11.7(1)(j); Australia-Singapore FTA, ch. 14, art. 7.1 (2003).

⁴⁹ Colombia-Israel FTA, annex-B, art. 3.

⁵⁰ EU-Japan EPA, arts. 18.1(2)(h), 18.16(7).

take into account the existing international standards,⁵¹ as well as criteria or guidelines of relevant international organizations or bodies⁵²—such as the APEC Privacy Framework and/or the OECD Guidelines on Transborder Flows of Personal Data (2013);⁵³ or to accord a high level of protection compatible with the highest international standards in order to ensure the confidence of e-commerce users.⁵⁴ In a handful of treaties, the Parties commit themselves to publishing information on the personal data protection they provide to users of e-commerce,⁵⁵ including how individuals can pursue remedies and how businesses can comply with any legal requirements.⁵⁶ Certain agreements place special emphasis on the transfer of personal data, stipulating that it shall only take place if necessary for the implementation, by the competent authorities, of agreements concluded between the Parties,⁵⁷ or that the countries need to have an adequate level of safeguards for the protection of personal data.⁵⁸ Some treaties add that the Parties will encourage the use of encryption or security mechanisms for the personal information of the users, and their dissociation or anonymization, in cases where said data is provided to third parties.⁵⁹

PTA Parties have also employed more binding options to protect personal information online. A first option is to consider the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records as an exception in specific chapters of the agreement—such as for trade

⁵¹ EU-Singapore FTA, art. 8.57(4); Argentina-Chile FTA, art. 11.5(1-2); Chile-Uruguay FTA, art. 8.7(2).

⁵² Australia-Indonesia FTA, art. 13.7(3); Australia-Peru FTA, art. 13.8(2); CETA, art. 16.4; Australia-Singapore FTA, ch. 14, art. 9.2 (2016); CPTPP, art. 14.8(2); Australia-China FTA, art. 12.8(2); Korea-Vietnam FTA, art. 10.6(2); Australia-Japan FTA, art. 13.8(2); EU-Ukraine AA, art. 139.2; EU-Georgia AA, art. 127.2; Australia-Korea FTA, art. 15.8; Mexico-Panama FTA, art. 14.8; Chile-Thailand FTA, art. 11.7(j); Colombia-Panama FTA, art. 19.6; Colombia-Costa Rica FTA, art. 16.6(1); Colombia-Korea FTA, arts. 12.1(2), 12.3; EU-Central America FTA, art. 201.2; Australia-Malaysia FTA, art. 15.8(2); ASEAN-Australia-New Zealand FTA, Ch. 10, art. 7.3; Australia-Chile FTA, art. 16.8; New Zealand-Thailand FTA, art. 10.5; Australia-Thailand FTA, art. 1106; Australia-Singapore FTA, ch. 14, art. 7.2 (2003).

⁵³ USMCA, art. 19.8(2).

⁵⁴ Armenia-EU CEPA, art. 197.2; Colombia-EU-Peru FTA, art. 162.2; Chile-EC AA, Chile-EC AA 119.2; CARIFORUM-EC EPA, art. 202.

⁵⁵ Brazil-Chile FTA, art. 10.8(4).

⁵⁶ USMCA, art. 19.8(5); Australia-Peru FTA, art. 13.8(4); Singapore-Sri Lanka FTA, art. 9.7(3); Australia-Singapore FTA, ch. 14, art. 9.4 (2016); Chile-Uruguay FTA, art. 8.7(3); CPTPP, art. 14.8(4); Singapore-Turkey FTA, art. 9.7(3).

⁵⁷ EU-Moldova AA, art. 13.2.

⁵⁸ Korea-Vietnam FTA, art. 10.6(2).

⁵⁹ Brazil-Chile FTA, art. 10.8(6); Argentina-Chile FTA, art. 11.5(6); Chile-Uruguay FTA, art. 8.7(5).

in services,⁶⁰ investment or establishment,⁶¹ movement of persons,⁶² telecommunications,⁶³ and financial services.⁶⁴ Certain agreements, mostly EU-led, have dedicated chapters on protection of personal data, including the principles of purpose limitation, data quality and proportionality, transparency, security, right to access, rectification and opposition, restrictions on onward transfers, and protection of sensitive data, as well as provisions on enforcement mechanisms, coherence with international commitments and cooperation between the Parties in order to ensure an adequate level of protection of personal data.⁶⁵ The 2018 USMCA was the first U.S.-led PTA to include such a provision that recognizes key principles of data protection.⁶⁶

A second option lets countries adopt appropriate measures to ensure privacy protection while allowing the free movement of data, establishing a criterion of “equivalence.” This has been largely the EU approach and to that end, Parties also commit to inform each other of their applicable rules and negotiate reciprocal, general, or specific agreements.⁶⁷ A third, but less used option, leaves the development of rules on data protection to a treaty body.

⁶⁰ Japan-Singapore FTA, art. 69.1(c).

⁶¹ Chile-EC AA, art. 135.1(e)(ii); Japan-Singapore FTA, art. 83.1(c)(ii).

⁶² Japan-Singapore FTA, art. 95.1(c)(ii).

⁶³ USMCA, art. 18.3(4); EU-Japan EPA, art. 8.44(4); Australia-Peru FTA, art. 12.4(4); Singapore-Sri Lanka FTA, art. 8.3(4); Argentina-Chile FTA, art. 10.3(4); Australia-Singapore FTA, art. 10.3(4) (2016); Singapore-Turkey FTA, art. 8.3(5); Japan-Mongolia FTA, annex 5, art. 3; Korea-Peru FTA, art. 13.3(4); Panama-US FTA, art. 13.2(4); Japan-Switzerland FTA, annex VI, art. IX(a); Nicaragua-Taiwan FTA, art. 13.02(4); Korea-Singapore FTA, art. 11.3(4); Morocco-US FTA, art. 13.2(4)(b); Chile-US FTA, art. 13.2(4).

⁶⁴ USMCA, annex 17-A; EU-Japan EPA, art. 8.63; EU-Vietnam FTA, art. 8.45; EU-Singapore FTA, art. 8.54(2); Australia-Peru FTA, art. 10.21; Armenia-EU CEPA, art. 185; CETA, art. 13.15(4); Australia-Singapore FTA, annex 9-B (2016); CPTPP, annex 11-B; Singapore-Turkey FTA, art. 10.12; Japan-Mongolia FTA, annex 4, art. 11; EU-Ukraine AA, art. 129.2; EU-Georgia AA, art. 118.2; ASEAN-Australia-New Zealand FTA, ch. 10, Annex on Financial Services, art. 7.2; Japan-Switzerland FTA, annex VI, art. VIII; EFTA-Colombia FTA, annex XVI—financial services, art. 8; EU-Moldova AA, art. 245; Chile-EU AA, art. 135.1(e)(ii).

⁶⁵ Cameroon-EC Interim EPA, ch. 6, arts. 61–65; CARIFORUM-EC EPA, ch. 6, arts. 197–201. Other agreements merely recognize principles for the collection, processing and storage of personal data such as: prior consent, legitimacy, purpose, proportionality, quality, safety, responsibility and information, but without developing this in detail: Argentina-Chile FTA, art. 11.2(5)(f) n.1; Chile-Uruguay FTA, art. 8.2(5)(f) n.3.

⁶⁶ USMCA, art. 19.8(3); *see also* below Section A.II.

⁶⁷ EU-Singapore FTA, art. 8.54(2); EU-Singapore FTA, Understanding 3—Additional Customs-Related Provisions, arts. 9.2, 11.1; EU-Ghana EPA, Protocol on Mutual Administrative Assistance on Custom Matters, art. 10; Bosnia and Herzegovina-EC SAA, Protocol 5 on Mutual Administrative Assistance on Custom Matters, art. 10.2; Algeria-EU Euro-Med Association Agreement, art. 45 & Protocol No. 7.

III. Different PTA Templates for Digital Trade Governance

As evident from the above overview, the regulatory environment for data flows has been shaped by PTAs. The United States has played a key role in this process and has sought to endorse liberal rules in implementation of its “Digital Agenda.”⁶⁸ The emergent regulatory template on digital issues is not however limited to U.S. agreements but has diffused and can be found in other PTAs, as evident from the above overview. Despite the fact there are still great variations in treaty language, certain distinct templates have been developed in recent years—one such template is shaped along the TPP model and now endorsed in the CPTPP and a number of subsequent agreements. The other and more recent model for digital trade has been promoted by the EU. The next sections look first at the CPTPP and its variations under the USMCA, the DTA, and the DEPA; then the new EU template and the Regional Comprehensive Economic Partnership (RCEP) are explored.

A. The U.S. Template

1. The Comprehensive and Progressive Agreement for Transpacific Partnership

The Comprehensive and Progressive Agreement for Transpacific Partnership (CPTPP) was agreed upon in 2017 between 11 countries in the Pacific Rim⁶⁹ and entered into force on December 30, 2018. Beyond the overall economic impact of the CPTPP, its chapter on e-commerce created the most comprehensive template in the landscape of PTAs and included several new features. Despite the fact that the United States dropped out of the agreement with the start of the Trump administration, the chapter still reflects U.S. efforts to secure obligations on digital trade and is a verbatim reiteration of the TPP chapter.

⁶⁸ See Sacha Wunsch-Vincent, *The Digital Trade Agenda of the US: Parallel Tracks of Bilateral, Regional and Multilateral Liberalization*, 58 *AUSSENWIRTSCHAFT* 7 (2003). 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 WTO-plus (going above the WTO commitments) and WTO-extra (addressing issues not covered by the WTO) provisions in the broader field of digital trade.

⁶⁹ Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, and Vietnam.

Particularly interesting for this chapter's discussion are the provisions found in the CPTPP e-commerce chapter that tackle the emergent issues of the data economy, previously unaddressed under the WTO framework. Most importantly, the CPTPP explicitly seeks to restrict the use of data protectionist 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." The soft language from U.S.–South Korea FTA on free data flows is now also framed 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."⁷⁰ The rule has a broad scope and most data transferred over the Internet is likely to be covered, although the word "for" may suggest the need for some causality between the flow of data and the business of the covered person; the explicit of personal data is also noteworthy.

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 information greater than are required to achieve the objective."⁷¹ These nondiscriminatory conditions are similar to the strict test formulated by Article XIV of the GATS and Article XX of the GATT 1994—a test that is aimed at balancing trade and non-trade interests by "excusing" certain violations (but is also extremely hard to pass, as we know from existing WTO jurisprudence).⁷² The CPTPP test differs from the WTO norms in one significant element: while there is a list of public policy objectives in GATT and GATS, the CPTPP provides no such enumeration and speaks merely of a "legitimate public policy objective."⁷³ This permits more regulatory autonomy for the CPTPP signatories but may lead to legal uncertainty. Further, it should be noted that the ban on localization measures is softened in regard to financial services and institutions.⁷⁴ An annex to the "Financial Services" chapter has a separate data transfer requirement,

⁷⁰ CPTPP, art. 14.11(2) (emphasis added).

⁷¹ *Id.* art. 14.11(3).

⁷² See, e.g., Henrik Andersen, *Protection of Non-Trade Values in WTO Appellate Body Jurisprudence: Exceptions, Economic Arguments, and Eluding Questions*, 18 J. INT'L ECON. L. 383 (2015).

⁷³ CPTPP, art. 14.11(3).

⁷⁴ For the definition of "a covered person," see *id.* art. 14.1, which excludes a "financial institution" and a "cross-border financial service supplier."

whereby certain restrictions on data flows may apply for the protection of privacy or confidentiality of individual records, or for prudential reasons.⁷⁵ Government procurement is also excluded.⁷⁶ Both exclusions are typical for all PTAs.

Another novel issue that the CPTPP addresses deals with 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.⁷⁷ This means that tailor-made products are excluded, as well as software used for critical infrastructure and those in commercially negotiated contracts.⁷⁸ This provision aims to protect software companies and address their concerns about loss of intellectual property, in particular trade secrets protection, or cracks in the security of their proprietary code; it may also be interpreted as a reaction to China's demands to access to source code from software producers selling in its market.

Overall, these provisions illustrate an interesting development because it is evident that they do not simply entail a clarification of existing bans on discrimination, nor do they merely set higher standards, as is commonly anticipated from trade agreements. Rather, they shape the regulatory space domestically. An important rule in this regard is in the area of privacy and 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."⁷⁹ 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

⁷⁵ 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."

⁷⁶ CPTPP, art. 14.8(3).

⁷⁷ *Id.* art. 14.17(2).

⁷⁸ *Id.*

⁷⁹ *Id.* art. 14.8(2).

privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy.”⁸⁰

Parties are also invited to promote compatibility between their data protection regimes, by essentially treating lower standards as equivalent.⁸¹ The goal of these norms can be interpreted as a prioritization of trade over privacy rights. This has been pushed by the United States during the TPP negotiations, as the United States subscribes to relatively weak and patchy protection of privacy. Timewise, this push came also at the phase, when the United States 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–U.S. Safe Harbor Agreement,⁸² which in hindsight had been a legitimate concern considering the 2020 follow-up decision of *Schrems II*.⁸³

Next to the data protection norms, the CPTPP includes also provisions on consumer protection⁸⁴ and spam control.⁸⁵ These are, however, fairly weak. The same is true for the newly introduced rules on cybersecurity. Article 14.16 CPTPP is non-binding and identifies a limited scope of activities for cooperation, in situations of “malicious intrusions” or “dissemination of malicious code” and capacity-building of governmental bodies dealing with cybersecurity incidents.

2. The United States–Mexico–Canada Agreement and the United States–Japan Digital Trade Agreement

The renegotiated NAFTA, which is now referred to as the “United States–Mexico–Canada Agreement” (USMCA), has a comprehensive e-commerce chapter that is now also properly titled “Digital Trade. “The chapter follows all critical lines of the CPTPP and goes beyond it. In particular, the USMCA

⁸⁰ *Id.* art. 14.8(2) n. 6.

⁸¹ *Id.* art. 14.8(5).

⁸² Case C-362/14, Maximilian Schrems v. Data Prot. Comm’r, EU:C:2015:650 (Oct. 6, 2015). Maximilian 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 United States. 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 United States—the so-called safe harbor scheme.

⁸³ The later EU–U.S. “privacy shield” arrangement, which replaced the Safe Harbor, was also rendered invalid by a recent judgment: Case C-311/18, Data Prot. Comm’r v. Facebook Ireland Ltd., Maximilian Schrems, ECLI:EU:C:2020:559 (July 16, 2020). A new Transatlantic Data Privacy Framework is currently under negotiation.

⁸⁴ CPTPP art. 14.17.

⁸⁵ *Id.* art. 14.14.

adheres to the CPTPP model with regard to data issues and ensures the free flow of data through a clear ban on data localization⁸⁶ and incorporates a hard rule on free information flows.⁸⁷ 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.⁸⁸

Beyond these similarities, the USMCA introduces some novelties. The first one is that the USMCA departs from the standard U.S. 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,”⁸⁹ 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).”⁹⁰ 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 accountability⁹¹ and aim to provide remedies for any violations.⁹² This is a key development because the USMCA may go beyond what the United States may have in its national laws on data protection and also reflects some of the principles the EU has advocated for in the

⁸⁶ USMCA, art. 19.12.

⁸⁷ *Id.* art. 19.11.

⁸⁸ *Id.* art. 19.11(2). 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.

⁸⁹ *Id.* art. 19.8(1).

⁹⁰ *Id.* art. 19.8(2). A footnote clarifies further that “For greater certainty, a Party may comply with the obligation in this paragraph by adopting or maintaining measures such as 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”.

⁹¹ *Id.* art. 19.8(3).

⁹² *Id.* art. 19.8(4)-(5).

domain of personal data protection. One may wonder whether this is a development caused by the so-called Brussels effect, whereby the EU “exports” its own domestic standards and renders them globally applicable,⁹³ or whether we are seeing a shift in U.S. privacy protection regimes.⁹⁴

Three further novelties 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”⁹⁵ and has become part of the ban on requirements for the transfer or access to source code in Article 19.16. 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.”⁹⁶ 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.⁹⁷ It also secures the application of Section 230 of the U.S. Communications Decency Act,⁹⁸ which insulates platforms from liability but has been recently under attack in many jurisdictions in the face of fake news and other negative developments related to platforms’ power.⁹⁹ While the safe harbor is very much to the benefit of U.S. tech companies, it has stirred controversies in the United States as well,¹⁰⁰ with

⁹³ ANU BRADFORD, *THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD* (2020).

⁹⁴ See Chander et al., *supra* note 13; Chander & Schwartz, *supra* note 14.

⁹⁵ USMCA, art. 19.1.

⁹⁶ *Id.* art. 19.17(2). Annex 19-A creates specific rules with the regard to the application of art. 19.17 for Mexico, in essence postponing its implementation for three years.

⁹⁷ On intermediaries’ liability, see, e.g., Sonia S. Katyal, *Filtering, Piracy, Surveillance and Disobedience*, 103 COLUM. J.L. & ARTS 401 (2009); Urs Gasser & Wolfgang Schulz, *Governance of Online Intermediaries: Observations from a Series of National Case Studies* (Berkman Ctr. for Internet & Soc’y, Research Publication No. 2015-5, 2015), <http://ssrn.com/abstract=2566364>.

⁹⁸ 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.

⁹⁹ See, e.g., Lauren Feine, *Big Tech’s Favorite Law Is under Fire*, CNBC (Feb. 19, 2020), <https://www.cnbc.com/2020/02/19/what-is-section-230-and-why-do-some-people-want-to-change-it.html>.

¹⁰⁰ For literature review, see, e.g., Mira Burri, *Fake News in Times of Pandemic and Beyond: An Enquiry into the Rationales for Regulating Information Platforms*, in *LAW AND ECONOMICS OF THE CORONAVIRUS CRISIS* (Klaus Mathis & Avishalom Tor, eds. 2022). See also the two recent Supreme Court cases *Gonzalez v. Google LLC*, 598 U.S. ____ (2023) and *Twitter Inc. v. Taamneh*, 598 U.S. ____ (2023).

Nancy Pelosi arguing against its inclusion.¹⁰¹ It remains to be seen whether future U.S. trade deals, struck under the Biden administration, will also include this limited platform's liability.

The third and rather liberal commitment of the USMCA parties regards 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 endeavor to ensure that the information is in a machine-readable and open format and can be searched, retrieved, used, reused, and redistributed."¹⁰² There is in addition an endeavor 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."¹⁰³

The U.S. approach toward digital trade issues has been confirmed also by the recent U.S.–Japan Digital Trade Agreement (DTA), signed on October 7, 2019, alongside the U.S.–Japan Trade Agreement.¹⁰⁴ The United States–Japan DTA arguably replicates almost all provisions of the USMCA and the CPTPP.¹⁰⁵ It incorporates the new USMCA rules on open government data,¹⁰⁶ source code,¹⁰⁷ and interactive computer services¹⁰⁸ but notably covering also financial and insurance services as part of the scope of agreement, thereby rendering its impact much broader. A new provision has been added

¹⁰¹ See, e.g., Brian Fung & Haley Byrd, *Nancy Pelosi Wants to Scrap Legal Protections for Big Tech in New Trade Agreement*, CNN (Dec. 5, 2019), <https://edition.cnn.com/2019/12/05/tech/pelosi-big-tech-legal-protections/index.html>. See also Han-Wei Liu, *Exporting the First Amendment Through Trade: The Global "Constitutional Moment" for Online Platform Liability*, 53 GEO. WASH. INT'L L. REV. 1 (2022).

¹⁰² USMCA, art. 19.18(2).

¹⁰³ *Id.* art. 19.8(3).

¹⁰⁴ For the text of the agreements, see Agreement between the United States of America and Japan Concerning Digital Trade, U.S.–Japan, Oct. 7, 2019, https://ustr.gov/sites/default/files/files/agreemnts/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf.

¹⁰⁵ Art. 7: Customs Duties; art. 8: Non-Discriminatory Treatment of Digital Products; art. 9: Domestic Electronic Transactions Framework; art. 10: Electronic Authentication and Electronic Signatures; art. 14: Online Consumer Protection; art. 11: Cross-Border Transfer of Information; art. 12: Location of Computing Facilities; art. 16: Unsolicited Commercial Electronic Messages; art. 19: Cybersecurity US–Japan DTA.

¹⁰⁶ US–Japan DTA, art. 20.

¹⁰⁷ *Id.* art. 17.

¹⁰⁸ *Id.* art. 18. 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 art. 18.

in regard to ICT goods that use cryptography. Article 21 DTA specifies that for such goods designed for commercial applications, neither party shall require a manufacturer or supplier of the ICT good as a condition to entering the market to (a) transfer or provide access to any proprietary information relating to cryptography; (b) partner or otherwise cooperate with a person in the territory of the Party in the development, manufacture, sale, distribution, import, or use of the ICT good; or (c) use or integrate a particular cryptographic algorithm or cipher.¹⁰⁹ This rule is similar to Annex 8-B, Section A.3 of the CPTPP chapter on technical trade barriers. It is a reaction to a practice by several countries, in particular China, that impose direct bans on encrypted products or set specific technical regulations that restrict the sale of encrypted products, and caters for the growing concerns of large companies, like IBM and Microsoft, that thrive on data flows with less governmental intervention.¹¹⁰

Other minor differences that can be noted when comparing with the USMCA are some things missing in the United States–Japan DTA—such as rules on paperless trading, net neutrality, and the mention of data protection principles.¹¹¹ The exceptions attached to the United States–Japan DTA refer to the WTO general exception clauses of Article XIV of the GATS and Article XX of the GATT 1994, whereby the parties agree to their *mutatis mutandis* application.¹¹² Further exceptions are listed with regard to security,¹¹³ prudential and monetary and exchange rate policy,¹¹⁴ and taxation,¹¹⁵ which are to be linked to the expanded scope of agreement including financial and insurance services.

3. The DEPA

The 2020 Digital Economy Partnership Agreement (DEPA) between Chile, New Zealand, and Singapore,¹¹⁶ all parties also to the CPTPP, should be

¹⁰⁹ *Id.* art. 21.3.

¹¹⁰ See Han-Wei Liu, *Inside the Black Box: Political Economy of the TPP's Encryption Clause*, 51 J. WORLD TRADE 309 (2017).

¹¹¹ Art. 15 merely stipulates that parties shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade and publish information on the personal information protection, including how: (a) natural persons can pursue remedies; and (b) an enterprise can comply with any legal requirements.

¹¹² US–Japan DTA, art. 3.

¹¹³ *Id.* art. 4.

¹¹⁴ *Id.* art. 5.

¹¹⁵ *Id.* art. 6.

¹¹⁶ For details and the text of the DEPA, see Digital Economy Partnership Agreement, Sing.-Chile-N.Z., June 12, 2020, <https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-concluded-but-not-in-force/digital-economy-partnership-agreement>.

mentioned as a new type of digital trade agreement, as it is not conceptualized as a purely trade deal 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 AI and digital inclusion. The agreement is also not a closed deal but one that is open to other countries,¹¹⁷ and the DEPA is meant to complement the WTO negotiations on e-commerce and build upon the digital economy work underway within APEC, the OECD, and other international forums. DEPA follows a modular approach, and 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 data¹¹⁸ (but not source code), and some of the United States–Japan DTA provisions, such as the one on ICT goods using cryptography,¹¹⁹ have been included too.

On the other hand, there are many other so far unknown for trade agreement rules that try to facilitate the functioning of the digital economy and enhance cooperation on key issues. For instance, Module 2 on business and trade facilitation includes next to the standard CPTPP-like norms,¹²⁰ 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.”¹²¹ 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.

With respect to AI, 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

¹¹⁷ DEPA, art. 16.2.

¹¹⁸ *Id.* art. 9.4.

¹¹⁹ *Id.* art. 3.4. The article also provides detailed definitions of cryptography, encryption, and cryptographic algorithm and cipher.

¹²⁰ *Id.* art. 2.2 (Paperless Trading); *id.* art. 2.3 (Domestic Electronic Transactions Framework).

¹²¹ *Id.* art. 2.2(5). “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. *Id.* art. 2.1.

would seek to follow internationally recognized principles or guidelines, including explainability, transparency, fairness, and human-centered values.¹²² 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.¹²³ Along this line of covering broader policy matters to create an enabling environment that is also not solely focused on and driven by economic interests, the DEPA deals with the importance of a rich and accessible public domain¹²⁴ and digital inclusion, which can cover enhancing cultural and people-to-people links, including between indigenous peoples, and improving access for women, rural populations, and low socioeconomic groups.¹²⁵

Overall, the DEPA is a unique and future-oriented project 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 attractivity as a form of enhanced cooperation on issues of data-driven economy has been confirmed by Canada's¹²⁶ and South Korea's¹²⁷ interest to join it. The DEPA's modular approach has been also followed in the Australia–Singapore Digital Economy Agreement, which is, however, still linked to the trade deal between the parties.¹²⁸

B. The Digital Trade Agreements of the European Union

Apart from the generic differences between the EU and the U.S. approaches to PTAs, the EU template in regard to digital trade is not as coherent as that

¹²² *Id.* art. 8.2(2)–(3).

¹²³ *Id.* arts. 8.3–8.4.

¹²⁴ *Id.* art. 9.2.

¹²⁵ *Id.* art. 11.2.

¹²⁶ Government of Canada, Global Affairs, Background: Canada's Possible Accession to the Digital Economy Partnership Agreement, Mar. 18, 2021, <https://www.international.gc.ca/trade-commerce/consultations/depa-apan/background-information.aspx?lang=eng>

¹²⁷ "South Korea Starts Process to Join DEPA," Oct. 6, 2021, <https://en.yna.co.kr/view/PYH20211006124000325>

¹²⁸ The DEA, which entered into force on Dec. 8, 2020, amends the Singapore–Australia FTA and replaces its Electronic Commerce chapter. See Australian Government, Department of Foreign Affairs and Trade, <https://www.dfat.gov.au/trade/services-and-digital-trade/australia-and-singapore-digital-economy-agreement>

of the United States.¹²⁹ It has also developed and changed over time. This can be explained by the EU's newly put stress on digital technologies as part of its innovation and growth strategy and with its new foreign policy orientation subsequent to the Lisbon Treaty, which includes PTAs as an essential strategic element.¹³⁰

The agreement with Chile (signed in 2002) was the first to include substantial e-commerce provisions but the language was still cautious and limited to soft cooperation pledges in the services chapter¹³¹ and in the fields of information technology, information society, and telecommunications.¹³² In more recent agreements, such as the EU–South Korea FTA (signed in 2009), the language is much more concrete and binding. It imitates some of the U.S. template provisions and confirms the applicability of the WTO Agreements to measures affecting electronic commerce, as well as subscribes to a permanent duty-free moratorium on electronic transmissions. The EU, as particularly insistent on data protection policies, has also sought commitment of its FTA partners to compatibility with the international standards of data protection.¹³³ 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.¹³⁴

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 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.¹³⁵ The EU has succeeded in deepening the privacy commitments and the CETA has a specific norm on trust and confidence in electronic commerce, which

¹²⁹ EU PTAs tend, for instance, to cover more WTO-plus areas but have less liberal commitments. For detailed analysis, see HENRIK HORN ET AL., *BEYOND THE WTO? AN ANATOMY OF EU AND US PREFERENTIAL TRADE AGREEMENTS* (2009), https://www.bruegel.org/wp-content/uploads/imported/publications/bp_trade_jan09.pdf.

¹³⁰ EU PREFERENTIAL TRADE AGREEMENTS: COMMERCE, FOREIGN POLICY, AND DEVELOPMENT ASPECTS (David Kleimann ed., 2013).

¹³¹ EU–Chile FTA, art. 102. 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”.

¹³² *Id.* art. 37.

¹³³ EU–South Korea FTA, art. 7.48.

¹³⁴ *Id.* art. 7.49.

¹³⁵ CETA, art. 16.5.

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.¹³⁶ Yet, there are no deep commitments on digital trade; nor there are any rules on data flows.

Overall, the EU has been cautious when inserting rules on data in its free trade deals and presently none of its treaties has such rules of binding nature. It is only recently that the EU has made a step toward such rules, whereby Parties have agreed to consider in future negotiations commitments related to cross-border flow of information. Such a clause is found in the 2018 EU–Japan EPA¹³⁷ and in the modernization of the trade part of the EU–Mexico Global Agreement. In the latter two agreements, the Parties commit to “reassess” within three years of the entry into force of the agreement, the need for inclusion of provisions on the free flow of data into the treaty. This signaled a repositioning of the EU on the issue of data flows, which is now fully endorsed in post-Brexit agreement with the U.K., the recently signed agreements with New Zealand and with Chile, and EU’s currently negotiated deals with Australia and Tunisia. These treaties include in their digital trade chapters norms that ensure the free flow of data. These newer commitments are, however, also linked with high levels of data protection.¹³⁸

The EU wishes to permit data flows only if coupled with the high data protection standards of its GDPR. In the aforementioned trade deals, as well as in the EU proposal for WTO rules on electronic commerce,¹³⁹ the EU follows a distinct model of endorsing and protecting privacy as a fundamental right. On the one hand, the EU and its partners seek to ban data localization measures and subscribe to a free data flow; but on the other hand, 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

¹³⁶ *Id.* art. 16.4.

¹³⁷ EU-Japan EPA, art. 8.81.

¹³⁸ See EUR. COMM’N, HORIZONTAL PROVISIONS FOR CROSS-BORDER DATA FLOWS AND FOR PERSONAL DATA PROTECTION IN EU TRADE AND INVESTMENT AGREEMENTS, in EU TRADE AND INVESTMENT AGREEMENT (2018), https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf.

¹³⁹ Eur. Union, *Joint Statement on Electronic Commerce: EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce, Communication from the European Union*, WTO Doc. INF/ECOM/22 (Apr. 26, 2019).

of trade,”¹⁴⁰ 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 afforded by the Parties’ respective safeguards.”¹⁴¹

The EU also wishes to retain the right to see how the implementation of the FTA with regard to data flows impacts 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.¹⁴² 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.”¹⁴³ The EU thus reserves ample regulatory leeway for its current and future data protection 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.¹⁴⁴

The new EU approach was first endorsed by the 2020 Trade and Cooperation Agreement (TCA) with the United Kingdom¹⁴⁵ that replicates all the above provisions, except for the explicit mentioning of data protection as a fundamental right—which can, however, be presumed, since the U.K. incorporates the European Convention on Human Rights (ECHR) through the Human Rights Act of 1998 into its domestic law (although the U.K. may be shifting away from the Strasbourg model post-Brexit¹⁴⁶). The

¹⁴⁰ See, e.g., draft EU-Australia FTA, art. 6(1) (emphasis added). The same wording is found in the EU-New Zealand FTA and the draft EU-Tunisia FTA.

¹⁴¹ See, e.g., *id.* art. 6(2). The same wording is found in the EU-New Zealand FTA and the draft EU-Tunisia FTA.

¹⁴² See, e.g., *id.* art. 5(2). The same wording is found in the EU-New Zealand FTA and the draft EU-Tunisia FTA.

¹⁴³ See, e.g., *id.* art. 2. The same wording is found in the EU-New Zealand FTA and the draft EU-Tunisia FTA.

¹⁴⁴ Svetlana Yakovleva, *Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy*, 74 U. MIAMI L. REV. 416, 496 (2020).

¹⁴⁵ 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, Dec. 30, 2020 [hereinafter TCA].

¹⁴⁶ See *Human Rights Act Reform: A Modern Bill of Rights – Consultation*, U.K. MINISTRY OF JUSTICE (July 12, 2022), <https://www.gov.uk/government/consultations/human-rights-act-ref>

rest of the EU digital trade template seems to include the issues covered by the CPTPP/USMCA model, such as software source code,¹⁴⁷ facilitation of electronic commerce,¹⁴⁸ online consumer protection,¹⁴⁹ spam,¹⁵⁰ and open government data,¹⁵¹ not including, however, a provision on non-discrimination of digital products, and excluding audio-visual services from the scope of the application of the digital trade chapter.¹⁵² It should also be underscored that the EU secures an essentially equivalent level of data protection in its PTA partners through the channel of adequacy decisions adopted unilaterally by the European Commission that are subject to monitoring and can be revoked in case that their requirements are not met.¹⁵³

Despite the confirmation of the EU's approach through the TCA¹⁵⁴ and the 2022 FTAs with New Zealand and Chile, it could be that the EU would tailor its template depending on the trade partner. For instance, the agreement with Vietnam,¹⁵⁵ which entered into force on August 1, 2020, has

orm-a-modern-bill-of-rights/human-rights-act-reform-a-modern-bill-of-rights-consultation; see also Conor Gearty, *The Human Rights Act Comes of Age*, 2 EUR. COMM'N H.R. L. REV. 117, 117–26 (2022).

¹⁴⁷ See TCA, *supra* note 185, art. 207. Again, with notable safeguards, specified in ¶¶ 2 and 3 of art. 207, including the general exceptions, security exceptions and a 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.

¹⁴⁸ See *id.* art. 205, 206.

¹⁴⁹ See *id.* art. 208.

¹⁵⁰ See *id.* art. 209.

¹⁵¹ See *id.* art. 210.

¹⁵² See *id.* art. 197.2.

¹⁵³ The European Commission has so far recognized Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the U.K. and Uruguay as providing adequate protection. With the exception of the U.K., these adequacy decisions do not cover data exchanges in the law enforcement sector. See European Commission, *Adequacy Decisions*, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en; see also Christopher Kuner, Article 45 Transfers on the Basis of an Adequacy Decision, in *THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A COMMENTARY*, 771–96 (Christopher Kuner et al., eds. 2020), <https://doi.org/10.1093/oso/9780198826491.003.0085>; Anastasia Choromidou, *EU Data Protection under the TCA: The UK Adequacy Decision and the Twin GDPRs*, 11 INT'L DATA PRIV. L. 388 (2021), <https://doi.org/10.1093/idpl/ipab021>.

¹⁵⁴ 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, 2020 O.J. (L 146) 10.

¹⁵⁵ Free Trade Agreement Between the European Union and the Socialist Republic of Viet Nam, E.U.-Viet., June 18, 2020, 2020 O.J. (L 186) 3, <http://trade.ec.europa.eu/doclib/press/index.cfm?id=1437>.

few cooperation provisions on electronic commerce as part of the services chapter, no dedicated chapter and importantly no reference to either data or privacy protection is made.¹⁵⁶ So while there is some certainty that in the deals with Australia and Tunisia, there will be digital trade provisions along the lines of the TCA, as well as in the FTAs with Chile and New Zealand, there is ambiguity as to the currently negotiated deals with India, Indonesia and the Association of Southeast Asian Nations (ASEAN).

C. The RCEP

An interesting and much anticipated development against the backdrop of the diverging EU and U.S. positions has been the recent Regional Comprehensive Economic Partnership (RCEP) between the ASEAN Members,¹⁵⁷ China, Japan, South Korea, Australia, and New Zealand. In terms of norms for the data-driven economy, the RCEP is certainly a less ambitious effort than the CPTPP and the USMCA, but still brings about significant changes to the regulatory environment and in particular to China's commitments in the area of digital trade. The RCEP provides only for conditional data flows, while preserving policy space for domestic policies, which may well be of data protectionist nature. The RCEP e-commerce includes a ban on localization measures¹⁵⁸ as well as a commitment to free data flows.¹⁵⁹ However, there are clarifications that give RCEP members a lot of flexibility, essentially undermining 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."¹⁶⁰ This essentially goes against any exceptions assessment, as we know it under WTO law, and triggers a self-judging mechanism.

¹⁵⁶ See Free Trade Agreement Between the European Union and the Socialist Republic of Viet Nam, E.U.-Viet., Mar. 30, 2020, 2020 O.J. (L 186) 63, https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/vietnam/eu-vietnam-agreement/texts-agreements_en.

¹⁵⁷ Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, and Vietnam.

¹⁵⁸ RCEP, art. 12.14.

¹⁵⁹ *Id.* art. 12.15.

¹⁶⁰ Emphases added.

In addition, subparagraph (b) of 12.14.3 says that the article 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.”¹⁶¹ 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. So, while in some senses, the RCEP’s e-commerce chapter is built upon the CPTPP’s framework, the treaty language is made more flexible in order to give the Parties leeway to adopt restrictive measures to digital trade and data flows.

IV. Conclusion

This chapter offers a mapping of developments in the area of digital trade governance with a deep dive on some more sophisticated templates that have been endorsed in recent years. It has become evident that PTAs have evolved into an important platform for rule-making in the area of digital trade, as well as that issues around data and data flows have moved to the center stage of trade negotiations. In the latter context, one could see that states have come up with new solutions that not only provide for legal certainty for data-driven businesses but also for policy space for the protection of vital public interests at home.

Yet, the question is still open as to whether this rule-making is adequate and sufficient to address the needs of the data-driven economy and our increasingly data-dependent societies. First, it must be acknowledged that preferential venues may not be ideal in this regard, as they create a complex and fragmented regulatory environment that does little to ensure seamless data flows, may be power driven and lacking in equality and equity. Furthermore, the above analysis revealed that the major stakeholders of the EU and the United States have adopted different approaches with regard to interfacing data protection and data-based innovation, and the EU as well as the RCEP Parties have been striving to carve out regulatory space and secure their digital sovereignty. This too may be suboptimal, as it does not provide for working reconciliation mechanisms and may undermine international

¹⁶¹ *Id.* art. 12.14.3(b) (emphasis added). The “essential security interest” language has been endorsed by China also in the framework of the WTO e-commerce negotiations.

cooperation in advancing the data-driven economy. The calls for more regulatory cooperation and legal innovation that manages the interfaces and trade-offs feasibly appear at this stage better answered by the new agreements dedicated to digital trade, such as the DEPA and have been driven by legal entrepreneurs, such as Singapore. These agreements could pave the path toward better solutions, albeit in parts in soft legal form, in the domain of digital trade governance, possibly also under the multilateral forum of the WTO.