www.jusletter-it.eu

Mira Burri

Switzerland in the Global Landscape of Digital Trade Regulation

While the landscape of digital trade regulation has changed profoundly in the last decade, Switzerland has not been a proactive actor in this ever more important domain of international economic law. The article sheds light on this mismatch. It first traces the evolution of global digital trade rule-making and outlines the positioning of major players. The article turns then to Switzerland and examines its extant network of FTAs and the provisions pertinent to the regulation of the digital economy, which are still few, albeit on the rise. The article concludes with some recommendations on the paths forward for Swiss external trade policy and its needed update to suit the demands of a global data-dependent economy and to adequately reflect Swiss economic and societal interests.

Category of articles: Articles
Field of law: E-Commerce, Economic Regulation

Citation: Mira Burri, Switzerland in the Global Landscape of Digital Trade Regulation, in: Jusletter IT 20 December 2023

ISSN 1664-848X, jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

Contents

A. Introduction

[1] The landscape of digital trade regulation has changed profoundly in the last decade due to the increased value associated with trading goods and services online, as well as distinct new phenomena that stem from the evolution of the data-driven economy. Switzerland has not been a proactive actor in this landscape and, for a highly industrialized and innovative economy, lags behind in regulatory entrepreneurship and geopolitical positioning in this new but ever more important domain of international economic law. The article seeks to shed light on this mismatch. It first traces the evolution of global digital trade rulemaking by exploring the regulatory models endorsed by free trade agreements (FTAs) that have become particularly distinctive and far-reaching after the 2018 Comprehensive and Progressive Trans-Pacific Partnership Agreement (CPTPP). The article seeks thereby to also outline the positioning of the major actors in the field with a focus on the United States (US), the European Union (EU) and China but also by looking at other proactive players, such as Singapore and the United Kingdom (UK). The article turns then to Switzerland and examines its extant network of FTAs and the provisions pertinent to the regulation of the data-driven economy, which, as will be shown, are only few, albeit on the rise. The article concludes with some recommendations on the paths forward for Swiss external trade policies that must be in many aspects updated to suit the demands of a global data-dependent economy and to adequately reflect Swiss economic and societal interests and values.

B. The global landscape of digital trade rulemaking

1. Overview and contemporary trends

[2] Despite the frequently shared understanding in the analyses of international law that states struggle to agree on common matters,[1] it is also true that the past two decades have witnessed a proliferation of rules and regulatory fora – of a soft and hard,[2] of a formal and informal nature.[3]

1 See e.g. Nico Krisch, «The Decay of Consent: International Law in an Age of Global Public Goods», *American Journal of International Law* 108 (2014), 1–40.

2 See e.g. Gregory C. Shaffer/Mark A. Pollack, «Hard vs. Soft Law: Alternatives, Complements, and Antagonists in International Governance», *Minnesota Law Review* 94 (2010), 706–799.

3 See e.g. Joost Pauwelyn/Ramses A. Wessel/Jan Wouters (eds), *Informal International Lawmaking* (Oxford: Oxford University Press, 2012).

With regard to trade, the lack of progress within the multilateral context of the World Trade Organization (WTO) has driven and continues to drive countries to seek other venues that better reflect their interests and allow for speedier solutions. Global trade law and policy reflect this regime shift[4] and can be distinguished by the great and growing number of preferential treaties, agreed upon bilaterally, regionally or between country groups.[5] Importantly, in many of these agreements «electronic commerce» or «digital trade»[6] issues have formed an essential part of the reasoning behind seeking the agreement, as well as of the content of the agreement itself.

[3] This evolution has been spurred by the progressively advancing digitization of economies and societies as a whole, as well as by the interlinked but more recently acknowledged importance of data.[7] In the context of trade policies, this has translated into efforts that ensure that data flows across borders, as data is embedded in a growing number of services and goods and there is a critical interdependence between cross-border data flows and digital growth and innovation – for instance, in the development of artificial intelligence (AI) or the Internet of Things (IoT).[8] The second reason behind the intensified digital trade rulemaking can be linked to the new set of regulatory questions that the use of data and its borderless nature[9] have opened – in particular those around data sovereignty and the protection of privacy, national security and other domestic values and interests.[10] Critical in this context, as the article reveals below, is that the emerging digital trade law seeks to address regulatory issues that go beyond classical WTO topics – such as reduction of tariffs or services liberalization, and ultimately calibrates the domestic regimes.

[4] As noted earlier, and despite the fact that the WTO law is in many ways relevant for online trade,[11] the contemporary regulatory for digital trade has been shaped by FTAs. Of the 432 FTAs signed between January 2000 and November 2023, 214 contain provisions relevant for e-

4 See e.g. J. P. Singh, *Negotiation and the Global Information Economy* (Cambridge: Cambridge University Press, 2008).

5 See e.g. WTO, World Trade Report 2011: The WTO and Preferential Trade Agreements: From Co-existence to Coherence (Geneva: World Trade Organization, 2011); Lillian Corbin/Mark Perry (eds), *Free Trade Agreements: Hegemony or Harmony* (Berlin: Springer, 2019).

6 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/Marie-Agnes Jouanjean, «Digital Trade: Developing a Framework for Analysis», *OECD Trade Policy Papers* 205 (2017). On the different definitions of digital trade, see Mira Burri/Anupam Chander, «What Are Digital Trade and Digital Trade Law?», *AJIL Unbound* 117 (2023), 99–103.

7 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/Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (New 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).

8 See e.g. Anupam Chander, «AI and Trade», in Mira Burri (ed), *Big Data and Global Trade Law* (Cambridge: Cambridge University Press, 2021), 115–127; Mira Burri, «The Impact of Digitization on Global Trade Law», *German Law Journal* 24 (2023), 551–573.

9 See e.g. Jennifer Daskal, «The Un-territoriality of Data», *The Yale Law Journal* 125 (2015), 326–398.

10 See e.g. Mira Burri, «Interfacing Privacy and Trade», *Case Western Journal of International Law* 53 (2021), 35–88; Anupam Chander/Paul M. Schwartz, «Privacy and/or Trade», *University of Chicago Law Review* 90 (2023), 49–135. For a fully-fledged analysis, see Anupam Chander/Haochen Sun (eds), *Data Sovereignty: From the Digital Silk Road to the Return of the State* (Oxford: Oxford University Press, 2023).

11 For an analysis of the WTO relevance to digital trade, see e.g. 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.

commerce/digital trade, and 122 have dedicated e-commerce/digital trade chapters,[12] with the significant jump in these commitments occurring in the past few years. Although the pertinent rules are still 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.[13] The new generation of Digital Economy Agreements (DEAs), which this article discusses below, is also indicative of the unfolding legal innovation and illustrates well the broader spectrum of regulatory matters that have become important in the data-driven economy and that countries seek to collectively address.

[5] Geopolitically, the surge in digital trade rulemaking can be well explained by the proactive role played by the US,[14] ever since the launch of its «Digital Agenda»[15] in 2001.[16] A great number of other countries have followed suit and adopted the US template[17] but some have also become proactive in their own right, with Singapore turning into the leading legal entrepreneur in the field in recent years. The EU, although to be reckoned with as a major actor in international economic law and policy, has interestingly been a latecomer into the digital trade rulemaking domain, as the article reveals below, but has now a clear and definitive stance. Developing countries have been also been somewhat slower in addressing digital trade issues. Yet, recent initiatives, such as the Regional Comprehensive Economic Partnership (RCEP), the Digital Trade Protocol of the Agreement Establishing the African Continental Free Trade Area (AfCFTA), as well as the forthcoming ASEAN negotiations towards a Digital Economy Framework Agreement (DEFA), illustrate well that there is a process of catching-up and that digital trade policies play an increasingly important role in regional integration.

2. Models of digital trade rulemaking and stakeholders' positioning

[6] In the following sections, the article looks at the new rules created in recent agreements through a detailed analysis of the most advanced electronic commerce/digital trade chapters[18]

12 This analysis is based on a dataset of all data-relevant norms in trade agreements (TAPED) administered by the University of Lucerne. For all data, see https://unilu.ch/taped.

13 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; Mira Burri, «A WTO Agreement on Electronic Commerce: An Inquiry into its Substance and Viability», *Georgetown Journal of International Law* 53 (2023), 565–625.

14 See Manfred Elsig/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.

15 US Congress, Bipartisan Trade Promotion Authority Act of 2001, H. R. 3005, 3 October 2001; see also Sacha Wunsch-Vincent, «The Digital Trade Agenda of the US», *Aussenwirtschaft* 1 (2003), 7–46; 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.

16 The US has reached since 2002 agreements with Australia, Bahrain, Chile, Morocco, Oman, Peru, Singapore, the Central American countries, Panama, Colombia, and South Korea that all contain critical, although with different depth of commitment, provisions in the broader field of digital trade. Newer and far-reaching agreements that this article discusses include the updated NAFTA and the Digital Technology Agreement with Japan.

17 For instance, agreements, such as Singapore-Australia, Thailand-Australia, New Zealand-Singapore, Japan-Singapore and South Korea-Singapore, are modelled along the US template. See also Elsig and Klotz, supra note 14.

18 Provisions relevant for digital trade can also be found in the chapters on cross-border supply of services (with particular relevance of the telecommunications, computer and related, audiovisual and financial services sectors) and in the chapters on IP protection. 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.

thus far – those of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), the United States-Mexico-Canada Agreement (USMCA), and the dedicated DEAs. 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 the depth of commitments and legal innovation in these treaties and to give a sense of the positions of the major stakeholders, on the other.

a. The Comprehensive and Progressive Agreement for Trans-Pacific Partnership

[7] The CPTPP was agreed upon in 2017 between eleven countries in the Pacific Rim[19] and entered into force on 30 December 2018. This «mega-regional» was originally conceived as the Transpacific Partnership Agreement (TPP) with the participation of the US, which, however, withdrew from the treaty negotiations with the start of the Trump administration. Nonetheless, the CPTPP e-commerce chapter is a verbatim reiteration of its TPP draft and in this sense reflects the US efforts under its updated «Digital 2 Dozen» agenda[20] to secure far-reaching obligations on digital trade.[21] Importantly for this article's discussion, the CPTPP electronic commerce chapter created at the time the most comprehensive template in the FTA landscape and deserves a closer look, as many of the subsequent agreements are compared with it, as to whether they go «CPTPP-plus» or «CPTPP-minus».[22]

[8] 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»[23] 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.[24] 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;[25] some additional exceptions are also specified.[26] The following provisions address, again as customarily, some of the leftovers of the 1998 WTO Work Programme on Electronic Commerce[27] 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

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

20 See United States Trade Representative, «The Digital 2 Dozen» (2016), https://ustr.gov/sites/default/files/Digital-2-Dozen-Final.pdf.

21 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.

22 See e.g. Mira Burri, «Trade Law 4.0: Are We There Yet?», *Journal of International Economic Law* 26 (2023), 90–100; Andrew D. Mitchell/Vandana Gyanchandani, «Convergence and Divergence in Digital Trade Regulation: A Comparative Analysis of the CP-TPP, RCEP, and eJSI», *South Carolina Journal of International Law and Business* 19 (2023), 98–150.

23 Article 14.2(2) CPTPP.

24 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 21, at 81–83.

25 Article 14.2(4) CPTPP.

26 Article 14.2(5) and (6) CPTPP.

27 WTO, Work Programme on Electronic Commerce, WT/L/274, 30 September 1998.

the non-discriminatory treatment of digital products,[28] which are defined broadly pursuant to Article 14.1.[29] Article 14.5 CPTPP is meant to shape the 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.[30] 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.[31] 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,[32] 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.[33]

[9] The remainder of the provisions found in the CPTPP electronic commerce chapter can be said to belong to a 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 that seek to keep data within states' territories, which have in recent years proliferated for a variety of reasons.[34] Specifically, Article 14.13(2) CPTPP 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 frames a hard rule on free data flows in the sense that: «[e]ach Party shall allow the cross-border transfer of information by electronic means, including personal

28 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.

29 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 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).

30 Article 14.5(2) CPTPP.

31 Article 14.9 CPTPP.

32 Article 14.6(1) CPTPP.

33 Article 14.6(2) CPTPP.

34 See e.g. United States International Trade Commission (USITC), *Digital Trade in the US and Global Economies*, Part 1, Investigation No 332–531 (Washington, DC: USITC, 2013); USITC, *Digital Trade in the US and Global Economies*, Part 2, Investigation No 332–540 (Washington, DC: USITC, 2014); United States Trade Representative (USTR), *2022 National Trade Estimate Report on Foreign Trade* (Washington, DC: USTR, 2022); Simon J. Evenett/Johannes Fritz, *Emergent Digital Fragmentation: The Perils of Unilateralism* (Brussels: CEPR Press, 2022).

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.

[10] Measures restricting data 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».[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 not entirely clear[39] – it can be linked to legal uncertainty, as well as to potentially unworkable safeguards for domestic constituencies, as pointed out by the New Zealand's Waitangi Tribunal with regard to the data governance rights of the Mori.[40] Lastly, it should be noted that the ban on localization measures is softened on financial services and institutions.[41] 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.[42] Government procurement is also excluded.[43]

[11] The CPTPP addresses other issues as well that were erstwhile novel – 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.[44] This means that tailor-made products are excluded, as well as software used for critical infrastructure and those in commercially negotiated contracts.[45] The aim of this provision is to protect software

35 Article 14.11(2) CPTPP.

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 For a great interpretation of this exception in light of existing WTO law and in comparison to other agreements, see Mitchell/Gyanchandani, supra note 22, at 117–122.

40 New Zealand's Waitangi Tribunal, Report on the Comprehensive and Progressive Agreement for Trans-Pacific Partnership, supra note 21, in particular at 132–142.

41 See the definition of «a covered person» (Article 14.1 CPTPP), which excludes a «financial institution» and a «cross-border financial service supplier».

42 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».

43 Article 14.8(3) CPTPP.

44 Article 14.17(2) CPTPP.

45 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 21, at 104–112.

companies and address their concerns about loss of intellectual property (IP) or cracks in the security of their proprietary code; it may also be interpreted as a reaction to China's demands for access to source code from software producers selling in its market.[46]

[12] 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».[47] 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».[48] Parties are also invited to promote compatibility between their data protection regimes, by essentially treating lower standards as equivalent.[49] 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.[50] Timewise, this push also came 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 the European Union (CJEU) that struck down the EU-US Safe Harbour Agreement.[51]

[13] Next to these important data protection provisions, the CPTPP also includes norms on consumer protection[52] and spam control,[53] as well as rules on cybersecurity. Article 14.16 is, however, non-binding and identifies a limited scope of activities for cooperation in the area of cybersecurity, in situations of «malicious intrusions» or «dissemination of malicious code», and capacity-building of governmental bodies dealing with cybersecurity incidents. Net neutrality

46 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.

47 Article 14.8(2) CPTPP.

48 Ibid., at footnote 6.

49 Article 14.8(5) CPTPP.

50 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/Daniel J. Solove, «Reconciling Personal Information in the United States and European Union», *California Law Review* 102 (2014), 877–916; also Burri (2021); Chander/Schwartz, both supra note 10.

51 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 being in adoption.

52 Article 14.17 CPTPP.

53 Article 14.14 CPTPP.

is another important digital economy topic that has been given specific attention in the CPTPP, although the so created rules are of a non-binding nature.[54]

[14] The 2023 accession of the UK to the CPTPP and pending applications by a number of countries, such as China, Taiwan, Ecuador and Costa Rica,[55] 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. In the following, the article discusses first at the USMCA and then looks at selected DEAs.

b. The United States-Mexico-Canada Agreement

[15] After the withdrawal of the US from the TPP, there was some uncertainty as to the direction the country 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». It 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,[56] bans customs duties on electronic transmissions[57] and binds the parties for non-discriminatory treatment of digital products.[58] Furthermore, it provides for a domestic regulatory framework that facilitates online trade by enabling electronic contracts,[59] electronic authentication and signatures,[60] and paperless trading.[61]

[16] The USMCA adheres to the CPTPP model also with regard to data issues and ensures the free flow of data through a clear ban on data localization[62] and a hard rule on free information flows.[63] 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

54 Article 14.10 CPTPP. 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. 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 a uniform approach with regard to net neutrality across the CPTPP countries.

55 See Jeffrey Schott, «Which Countries Are in the CPTPP and RCEP Trade Agreements and Which Want in?», Peterson Institute for International Economics blog, 27 July 2023, at: https://www.piie.com/research/piie-charts/which-countries-are-cptpp-and-rcep-trade-agreements-and-which-want.

56 Article 19.2 USMCA.

57 Article 19.3 USMCA.

58 Article 19.4 USMCA.

59 Article 19.5 USMCA.

60 Article 19.6 USMCA.

61 Article 19.9 USMCA.

62 Article 19.12 USMCA.

63 Article 19.11 USMCA.

trade; and the restrictions on transfers of information are not greater than necessary to achieve the objective.[64]

[17] 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»[65], 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)».[66] 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,[67] and aim to provide remedies for any violations.[68] This is interesting because it may go beyond what the US has in its national laws on data protection (at least so far[69]) 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», whereby the EU «exports» its own domestic standards and they become global,[70] or whether we are seeing a shift in US privacy protection regimes as well.[71]

[18] 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»[72] and has become part of the ban on requirements for the transfer or access to source code in Article 19.16.[73] 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 ser-

64 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.

65 Article 19.8(1) USMCA.

66 Article 19.8(2) USMCA.

67 Article 19.8(3) USMCA.

68 Article19.8(4) and (5) USMCA.

69 Chander/Schwartz, supra note 10.

70 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).

71 See Anupam Chander/Margot E. Kaminski/William McGeveran, «Catalyzing Privacy Law», *Minnesota Law Review* 105 (2021), 1733–1802.

72 Article 19.1 USMCA.

73 On the expansion of the scope of the source code provision, see New Zealand's Waitangi Tribunal, supra note 21, at 104–112.

vice, except to the extent the supplier or user has, in whole or in part, created, or developed the information».[74] 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,[75] which insulates platforms from liability[76] but has been recently under attack in many jurisdictions (including in the US[77]) in the face of fake news and other negative developments related to platforms' power.[78]

[19] 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]

[20] The US approach towards digital trade issues has been confirmed by the US-Japan Digital Trade Agreement (DTA), signed on 7 October 2019, alongside the US-Japan Trade Agreement.[83]

---

74 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.

75 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.

76 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.

77 See in particular the two recent Supreme Court cases: *Gonzalez v. Google LLC*, 598 U. S. ____ (2023) and *Twitter Inc. v. Taamneh*, 598 U. S. ____ (2023). See also Han-Wei Liu, «Exporting the First Amendment through Trade: The Global ‹Constitutional Moment› for Online Platform Liability», *George Washington International Law Review* 53 (2022), 1–56; Mira Burri, «Digital Trade and Human Rights», *AJIL Unbound* 117 (2023), 110–115.

78 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/Avishalom Tor (eds), *Law and Economics of the Coronavirus Crisis* (Berlin: Springer, 2022), 31–58.

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.

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 the agreement. In the current WTO negotiations on electronic commerce under the 2019 Joint Initiative,[88] the US had initially endorsed an ambitious template, which was essentially a compilation of the USMCA and the DTA.[89] As to the future US position on digital trade, there appears at this point of time to be some uncertainty. First, it is unclear whether the US would join and/or try to renegotiate the CPTPP, as there is some uncertainty moving towards the end of the Biden administration, the US appears to engage in broader and less binding cooperation initiatives,[90] such as the Indo-Pacific Economic Framework for Prosperity (IPEF).[91] Second and more importantly for the WTO context, the US has recently announced that it will disengage in the negotiations on the topics of data flows, data localization and source code, as it needs «policy space» for a digital trade rethink.[92]

c. Digital Economy Agreements

[21] The increased preoccupation of policymakers with digital trade issues can be perhaps best exemplified by the emergent 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 DTA; 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 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

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 For a discussion of the JI negotiations, see Burri (2023), supra note 13; Yasmin Ismail, *The Evolving Context and Dynamics of the WTO Joint Initiative on E-commerce: The Fifth-Year Stocktake and Prospects for 2023* (Geneva: International Institute for Sustainable Development and CUTS International, 2023).

89 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.

90 See e.g. Mitchell/Gyanchandani, supra note 22.

91 The US launched the IPEF in May 2022 with Australia, Brunei Darussalam, Fiji, India, Indonesia, Japan, the Republic of Korea, Malaysia, New Zealand, Philippines, Singapore, Thailand and Vietnam. For details, see https://ustr.gov/trade-agreements/agreements-under-negotiation/indo-pacific-economic-framework-prosperity-ipef.

92 See Inside US Trade, «US to End Support for WTO E-commerce Proposals, Wants ‹Policy Spaceguilsinglright for Digital Trade Rethink», 24 October 2023.

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 a representative of this latter category and as a model of innovative digital trade rulemaking.

[22] The 2020 DEPA between Chile, New Zealand, and Singapore,[93] 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[94] 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.[95] 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 (Module 14); dispute settlement (Module 15); and some final provisions on amendments, entry into force, accession and withdrawal (Module 16).

[23] 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[96] (but not source code), and some of the US-Japan DTA provisions, such as the one on ICT goods using cryptography,[97] 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,[98] 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».[99] Parties have also touched upon other important issues around digital trade facilitation, such as electronic invoic-

93 For details and the text of the DEPA, see: https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement-depa/depa-text-and-resources/#bookmark0.

94 Article 16.2 DEPA.

95 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.

96 Article 9.4 DEPA.

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

98 Article 2.2: Paperless Trading; Article 2.3: Domestic Electronic Transactions Framework.

99 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).

ing (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.[100] 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.[101] 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[102] 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.[103]

[24] Overall, the DEPA is a unique project[104] 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[105] and South Korea's[106] 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. Geopolitically, the DEAs show that there is a shift in the landscape of digital trade rulemaking from traditional digital trade legal demanders, such as notably the US, to new actors. The DEAs are predominantly being developed by dynamic countries seeking to capitalize on the economic potential of the digital economy, and Singapore in particular (as party to all but one DEA) has become the leader in this effort with the UK following suit and imitating this proactive stance.[107]

100 Article 8.2(2) and (3) DEPA.

101 Articles 8.3 and 8.4 DEPA.

102 Article 9.2 DEPA.

103 Article 11.2 DEPA.

104 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.

105 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.

106 «South Korea Starts Process to Join DEPA», 6 October 2021, available at: https://en.yna.co.kr/view/PYH20211006124000325.

107 See Emily Jones/Beatriz Kira/Rutendo Tavengerwei, «Norm Entrepreneurship in Digital Trade: The Singapore-led Wave of Digital Trade Agreements», Working Paper (2023) (on file with the author).

d. EU's approach to digital trade regulation

[25] The EU has been a relatively late mover on digital trade issues, despite having a wide-ranging domestic framework for the regulation of the data economy, 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[108] and in the fields of information technology, information society and telecommunications.[109] 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.[110] The EU, as particularly insistent on data protection policies, has also sought commitment from its FTA partners to seek compatibility with the international standards of data protection.[111]

[26] 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.[112] 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.[113] Yet, there are no deep commitments on digital trade; nor there are any rules on data and data flows.[114]

[27] 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)[115] 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 and the

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

109 Article 37 EU-Chile FTA.

110 Article 7.49 EU-South Korea FTA.

111 Article 7.48 EU-South Korea FTA.

112 Article 16.5 CETA.

113 Article 16.4 CETA.

114 See e.g. Wolfe, supra note 74.

115 Article 8.81 EU-Japan EPA.

2023 agreement with Chile. These FTAs' digital trade chapters include norms on data and data localization bans. This repositioning and newer commitments are, however, also linked with high levels of data protection.[116]

[28] The EU wishes to permit data flows only if coupled with the high standards of its General Data Protection Regulation (GDPR)[117] 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»,[118] 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».[119] 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.[120] 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».[121] 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.[122]

[29] The new EU approach was first confirmed by the post-Brexit Trade and Cooperation Agreement (TCA) with the United Kingdom,[123] 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

116 See European Commission, Horizontal Provisions for Cross-Border Data Flows and for Personal Data Protection in EU Trade and Investment Agreements, February 2018.

117 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].

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

119 See e.g. Article 6(2) draft EU-Australia FTA. The same wording is found in the EU-New Zealand, EU-Chile and the draft EU-Tunisia FTA.

120 See e.g. Article 5(2) draft EU-Australia FTA. The same wording is found in the EU-New Zealand, EU-Chile and the draft EU-Tunisia FTA.

121 See e.g. Article 2 draft EU-Australia FTA. The same wording is found in the EU-New Zealand, EU-Chile and the draft EU-Tunisia FTA.

122 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.

123 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.

the Human Rights Act of 1998 into its domestic law.[124] 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 and may create problems for data flows going across the Channel.

[30] 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,[125] facilitation of electronic commerce,[126] online consumer protection,[127] spam[128] and open government data;[129] 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.[130] This TCA template is also the one that the EU has endorsed under the WTO electronic commerce negotiations.[131] The EU is also engaging in other, not strictly trade-related, channels to further its digital sovereignty (including important technological aspects) and ensure the protection of its citizens' rights. In the latter sense, this occurs through the negotiation and adoption of adequacy decisions with countries that must secure an equivalent level of personal data protection (Switzerland being notably one of these countries).[132] The former channel is through the newly endorsed digital partnership agreements, such as those with Japan and Singapore,[133] that address issues around semiconductors, digital trust, standards, digital trade facilitation, digital skills for workers, and the digital transformation of businesses and public services.

e. The Regional Comprehensive Economic Partnership

[31] An interesting development against the backdrop of the diverging, at least on data flows, EU and US positions has been the Regional Comprehensive Economic Partnership (RCEP) signed on 15 November 2020 between the ASEAN Members,[134] China, Japan, South Korea, Australia and

124 See e.g. Kristina Irion/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.

125 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.

126 Articles 205 and 206 TCA.

127 Article 208 TCA.

128 Article 209 TCA.

129 Article 210 TCA.

130 Article 197(2) TCA.

131 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.

132 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 United Kingdom and Uruguay as providing adequate protection. The US adequacy decision was struck down pursuant to the *Schrems* judgments (see supra note 51).

133 See https://digital-strategy.ec.europa.eu/en/policies/partnerships. See also Nicolas Köhler-Suzuki, «Mapping the EU's Digital Trade: A Global Leader Hidden in Plain Sight?», *Jacques Delors Institute Policy Paper* 292 (2023).

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

New Zealand and in force since 1 January 2022.[135] 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.

[32] With regard to trade facilitation, RCEP includes provisions on paperless trading,[136] on electronic authentication and electronic signatures.[137] On paperless trading, the RCEP Members avoid entering into binding commitments. They, instead, commit to «works toward», «endeavor», or «cooperate».[138] The norms on accepting the validity of 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[139] and cybersecurity[140] 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,[141] unsolicited commercial electronic messages,[142] and a framework governing electronic transactions that takes into account international instruments,[143] as well as commit to transparency.[144]

[33] 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,[145] as well

135 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/.

136 Article 12.5 RCEP.

137 Article 12.6 RCEP.

138 Article 12.5 RCEP.

139 Article 12.8 RCEP.

140 Article 12.13 RCEP.

141 Article 12.7 RCEP.

142 Article 12.9 RCEP.

143 Article 12.10 RCEP.

144 Article 12.12 RCEP.

145 Article 12.14 RCEP.

as a commitment to free data flows,[146] 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».[147] Article 12.15 RCEP 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.

[34] Other provisions contained in the RCEP electronic commerce chapter include the establishment of a dialogue on electronic commerce[148] and a provision on dispute settlement,[149] which is separate from the general RCEP's dispute settlement.[150] Noteworthy are also some things that are different or missing from the RCEP: in comparison to the CPTPP model, RCEP conditions the custom duties moratorium on the prevailing WTO practice; does not include 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,[151] and not engaging in commitments on data flows. It is also interesting to contemplate how China's wish to join the CPTPP and DEPA would impact the WTO negotiations as well as largely the landscape of digital trade rulemaking – perhaps tilting it towards national security and other carve-outs that diminish the value of the made commitments and prejudice legal certainty. Some authors think, on the other hand, that the RCEP is a good model that reflects domestic policy preferences, while opening up for digital trade. It has been argued that this pragmatic and incremental approach should not be viewed as inferior but rather as one that addresses well the existing variations in digital development levels across countries, «eventually leading to meaningful consensus-building and long-term engagement in complex areas of digital regulation».[152]

C. Switzerland's FTAs and their relevance for digital trade

[35] In addition to the European Free Trade Association (EFTA) Convention and the Free Trade Agreement with the EU of 1973, Switzerland has an extensive network of preferential agreements

146 Article 12.15 RCEP.

147 Emphases added. On the different definitions of «essential security interests», see Mitchell/Gyanchandani, supra note 22.

148 Article 12.16 RCEP.

149 Article 12.17 RCEP.

150 Chapter 12 RCEP. There is a possibility for this to change after a review of the chapter (Article 12.17(3) RCEP).

151 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.

152 See Neha Mishra/Ana Maria Palacio Valencia, «Digital Services and Digital Trade in the Asia Pacific: An Alternative Model for Digital Integration?», *Asia Pacific Law Review* 31 (2023), 489–513.

comprising 34 FTAs with 45 partners.[153] Most of its agreements have been concluded together with its EFTA partners (Norway, Iceland and Liechtenstein). But Switzerland has also completed bilateral agreements in its own right – so far with the Faroe Islands, Japan, China and the UK. With regard to these deals, it can be broadly maintained that Switzerland has followed the EU model in most essential aspects, also because the rest of the EFTA members except for Switzerland are part of the European Economic Area (EEA) and thus bound by the EU *acquis*.[154] Yet, there are some clear differences too. The most striking one is that, in contrast to the EU, Switzerland has not formulated and implemented a distinct strategy with regard to digital trade in its current FTAs. Most of the existing agreements have no discrete electronic commerce chapters. Of all its FTAs that it has concluded since 2000 up to date, only two agreements have an electronic commerce chapter, while eleven out of the 34 Swiss FTAs have electronic commerce provisions.[155]

[36] In Switzerland's EFTA deals, there are some relevant provisions but these are predominantly of soft law nature. In this sense, the FTA with the Member States of the Co-operation Council for the Arab States of the Gulf (GCC),[156] which entered into force in 2014, includes an annex to Article 9.3 «Electronic Commerce» that merely includes 3 provisions with regard to recognizing (a) the economic growth and opportunities that electronic commerce in goods and services provides, in particular for businesses and consumers, as well as the potential for enhancing international trade; (b) the importance of avoiding barriers to the use and development of electronic commerce in goods and services; and (c) the need to create an environment of trust and confidence for users of electronic commerce;[157] combined with provisions on exchange of information[158] and certain organizational channels, so as to enable to exchange of information.[159] In the same way, the FTA with Colombia includes a generic provision recognizing the importance of electronic commerce[160] with a reference to an annex of low normative value.[161] The same is true about the 2011 EFTA FTA with Peru, which essentially contains identical norms.[162] The 2014 agreement with the Central American states[163] duplicates these provisions[164] but includes a pledge whereby parties confirm their current practice under the WTO moratorium of not imposing customs duties on electronic transmissions[165] – again a provision with no real legal effect. The EFTA FTA with

153 For an overview of agreements and partners, see State Secretariat for Economic Affairs (SECO), «Free trade partners of Switzerland», at: https://www.seco.admin.ch/seco/en/home/Aussenwirtschaftspolitik_Wirtschaftliche_-Zusammenarbeit/Wirtschaftsbeziehungen/.

154 See e.g. Matthias Oesch, «Wird die handelspolitische Autonomie der EFTA-Staaten überschätzt?», *EuR*, Beiheft 1 (2020), 329–355.

155 EFTA-Mexico FTA (2001); Chile-EFTA FTA (2004); Colombia-EFTA FTA (2011); EFTA-Peru FTA (2011); EFTA-Ukraine FTA (2012); Central American States-EFTA FTA (2014); GCC-EFTA FTA (2014); China-Switzerland FTA (2014); EFTA-Georgia FTA (2018); Ecuador-EFTA FTA (2020); EFTA-Turkey Upgraded FTA (2021).

156 The GCC includes six Middle Eastern countries – Saudi Arabia, Kuwait, the United Arab Emirates, Qatar, Bahrain and Oman.

157 Annex XVI, Article 1 EFTA-GCC FTA.

158 Annex XVI, Article 2 EFTA-GCC FTA.

159 Annex XVI, Article 3 EFTA-GCC FTA.

160 Article 1.8 EFTA-Columbia FTA.

161 Annex I EFTA-Columbia FTA. The Annex contains essentially the same recognition and exchange of information provisions as the EFTA-GCC FTA.

162 Article 1.8 and Annex I EFTA-Peru FTA.

163 Costa Rica, Guatemala and Panama.

164 Article 1.8 and Annex II EFTA-Central America FTA.

165 Annex II, Article 2 EFTA-Central America FTA.

Turkey modernized in 2018 includes for the first time more substantive and detailed provisions in an annex to the agreement. It covers in particular a temporary customs duties moratorium[166]; electronic signatures and certification[167]; online consumer protection[168]; norms on personal data protection and spam[169]; paperless trading and e-commerce cooperation.[170] It should be noted that the rest of the EFTA deals, including the 2021 agreement with Indonesia, have no provisions on electronic commerce.[171]

[37] The 2023 EFTA agreement with Moldova changes this cautious practice however and has a fully-fledged e-commerce chapter, which is the first implementation of the template agreed among the EFTA members. Chapter 5 reflects the structure and the substance of the EU model and covers: Definitions;[172] Scope[173]; General Provisions[174]; Right to regulate[175]; Custom duties[176]; Electronic authentication, trust services and contracts by electronic means[177]; Paperless trade administration[178]; Open internet access[179]; Online consumer trust[180]; Unsolicited commercial electronic messages[181]; Cross-border data flows[182]; Electronic payments and invoicing[183]; Protection of personal data and privacy[184]; Transfer of and access to source code[185]; and Cooperation.[186] Articles 5.15 and 5.16 include general and security exceptions respectively and provide for a *mutatis mutandis* application of the corresponding WTO exceptions.[187] In contrast to the EU model, it is noteworthy that the right to regulate is more succinctly formulated in that: «The

166 Annex XIII, Article 4 EFTA-Turkey FTA.

167 Annex XIII, Article 5 EFTA-Turkey FTA.

168 Annex XIII, Article 6 EFTA-Turkey FTA.

169 Annex XIII, Articles 7 and 8 EFTA-Turkey FTA.

170 Annex XIII, Articles 9 and 10 EFTA-Turkey FTA.

171 Some relevance can be found in the Annex on Financial Services, where Article 7 clarifies with regard to data transfers that: «The Parties confirm that pursuant to Article 7 (Transfers of Information and Processing of Information), and for the purposes of Annex XIV (Financial Services), the term ‹rightsguilsinglright includes the rights to require a financial services supplier in its territory to comply with domestic laws and regulations requiring local data management and storage or local processing».

172 Article 5.1 EFTA-Moldova FTA.

173 Article 5.2 EFTA-Moldova FTA.

174 Article 5.3 EFTA-Moldova FTA.

175 Article 5.4 EFTA-Moldova FTA.

176 Article 5.5 EFTA-Moldova FTA.

177 Article 5.6 EFTA-Moldova FTA.

178 Article 5.7 EFTA-Moldova FTA.

179 Article 5.8 EFTA-Moldova FTA.

180 Article 5.9 EFTA-Moldova FTA.

181 Article 5.10 EFTA-Moldova FTA.

182 Article 5.11 EFTA-Moldova FTA.

183 Article 5.12 EFTA-Moldova FTA.

184 Article 5.13 EFTA-Moldova FTA.

185 Article 5.14 EFTA-Moldova FTA.

186 Article 5.15 EFTA-Moldova FTA.

187 Under Article XX of the GATT 1994 and Article XIV of the GATS (general exceptions) and Article XXI of the GATT 1994 and Article XIV*bis* of the GATS (security exceptions). Under Article 5.11(2), there is an additional built-in security exception for Norway: «Between Norway and the Republic of Moldova, nothing in this Article shall be construed to prevent Norway or the Republic of Moldova from taking any action which it considers necessary for the protection of its essential security interests».

Parties reaffirm the right to regulate in the area of electronic commerce in conformity with this Chapter to achieve legitimate policy objectives».[188]

[38] The position of Switzerland in its own bilateral agreements is also important. The agreement with Japan (in force since 2009[189]) contains a detailed chapter on electronic commerce.[190] It is framed along the EU model – however, with a few discrete specificities that appear even a bit exotic when compared to existing treaty language across FTAs. The common features relate to the scope of the agreement,[191] provisions on electronic signatures,[192] paperless trade administration,[193] consumer protection online,[194] as well as a temporary customs duties moratorium.[195] The non-discrimination obligation included, which is atypical for an EU deal, may have a broader scope, as it is linked to a liberal definition of «digital products» as products such as computer programmes, texts, plans, designs, video, images and sound recordings or any combinations thereof, that are digitally encoded and transmitted electronically;[196] there is also a specific non-discrimination provision for services, which is however not framed as an extension of the most-favoured nation (MFN) and/or the national treatment (NT) obligation but merely ensures technological neutrality in that services supplied by electronic services are not discriminated against vis-à-vis services provided by other means. Finally, the electronic commerce chapter includes a comprehensive cooperation pledge that encompasses (a) data privacy; (b) fight against unsolicited commercial messages; (c) consumer confidence in electronic commerce; (d) cybersecurity; (e) IP; (f) electronic government; and (g) public morals, in particular ethics for young generations.[197] It also makes reference to the need to include multistakeholder approaches in the governance of digital trade, as well as cooperation on efforts to develop the international framework for electronic commerce.[198] This is an innovative feature of the Swiss FTA with Japan, which relates to broader issues of Internet governance. Overall, the digital trade commitments under the Switzerland-Japan FTA, although to be deemed of low normative effect, show Switzerland's first real engagement with electronic commerce rules, without touching upon the more critical issues of the advanced data-driven economy. Their inclusion can be attributed to Japan's proactive stance[199] rather than Switzerland's. The more recent agreement with China, which entered into force in 2014, lacks entirely an electronic commerce chapter.[200] The same is true for the post-Brexit agreement with the UK, which was at that point of time a mere continuity trade agreement

188 Article 5.4 EFTA-Moldova FTA.

189 Abkommen über Freihandel und wirtschaftliche Partnerschaft zwischen der Schweizerischen Eidgenossenschaft und Japan vom 19. Februar 2009 (SR 0.946.294.632) [hereinafter Switzerland-Japan FTA].

190 Chapter 8 Switzerland-Japan FTA.

191 Article 70 Switzerland-Japan FTA.

192 Article 78 Switzerland-Japan FTA.

193 Article 79 Switzerland-Japan FTA.

194 Article 80 Switzerland-Japan FTA.

195 Article 76 Switzerland-Japan FTA.

196 Switzerland-Japan FTA, Article 72(a). An additional note specifies that for the purposes of this Chapter, digital products do not include those that are fixed on a carrier medium. These are covered by Chapter 2 on trade in goods.

197 Article 82 Switzerland-Japan FTA.

198 Article 82(4) Switzerland-Japan FTA.

199 Since then, Japan has signed seven FTAs with separate electronic or digital trade chapters, including the DTA with the US.

200 China, on the other hand, up to 2022, has concluded six FTAs with separate electronic commerce chapters, including the update of previous deals with trading partners.

that sought to replicate as far as possible the trade arrangements between Switzerland and the EU.[201]

[39] One might argue that, although Switzerland's FTAs have few digital trade provisions in dedicated chapters (except for the EFTA-Moldova FTA), the rest of the treaties' language, especially in the services and the IP chapters, includes digital trade-relevant provisions. This is however not strictly the case. In terms of services commitments, Switzerland has above all sought to secure that its regulatory space in some digital trade domains – notably audio-visual services – is well preserved. It not only lists all excluded sub-sectors in a detailed manner that mirrors the current situation in Switzerland but secures some wiggle-room for the adoption of measures in the future too. These are defined on the one hand as a discrete category of «new services» but also as an additional qualification in a number of sectors. So, for instance, Switzerland has reserved the right to maintain, modify or adopt any measures restricting market access and national treatment with respect to broadcasting services.[202] There is also a new generic category introduced – that of «Internet-based services» – for which Switzerland reserves its right to introduce measures with respect to the protection of youth or to the prevention of addiction or compulsive behaviour and other mental health hazards.[203] Even in the IP chapters, while there is a reference to the WIPO Internet Treaties, no obligations with regard to the application of technological protection matters and/or the liability of internet service providers (ISPs) are spelled out. This is true also for recent FTAs, such as those with Hong Kong, with Bosnia and Herzegovina and Indonesia (in force since 2012, 2015 and 2021 respectively). One explanation for this may be that these deals are the result of the joint negotiations with the EFTA partners and must reflect their common stance. Still, it is a pity that Switzerland has not updated its IP chapters in a way that reflects the implications of the digital environment. This also is not congruent with developments in the US and EU agreements[204] and the Swiss domestic framework introduced with the 2020 Swiss Copyright Act. On the other hand, it can be argued that despite the lack of new «digitized» rulemaking, Switzerland has a fairly open digital economy[205] and corresponding far-reaching commitments under the WTO's General Agreement on Trade in Services (GATS) for key digital trade sectors, such as telecommunication, computer and related and financial services, which at times go farther than those of digital champions like the US or Singapore.

D. Concluding remarks and outlook

[40] The above enquiry into 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 DEAs are quite impressive, and there is a strand of legal innovation that seeks to tackle the multitude of issues raised in the context of a global data-dependent economy. The regulatory

201 See UK Department for Business and Trade, *UK-Switzerland Free Trade Agreement: The UK's Strategic Approach* (London: Department for Business and Trade, 2023); also Jones/Kira/Tavengerwei, supra note 107.

202 EFTA-Hong Kong FTA, Annex X, List of Reservations and Commitments: Switzerland, at Section 31.

203 Ibid., at Section 100.

204 See e.g. Burri (2017), supra note 18 (showing convergence tendencies across EU and US IP chapters).

205 See e.g. the ranking of Switzerland under the OECD Services Trade Restrictiveness Index (STRI), available at: https://www.oecd.org/trade/topics/services-trade/documents/oecd-stri-country-note-che.pdf.

environment is however still 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. Although this article did not discuss the plurilateral negotiations under the WTO Joint Initiative on Electronic Commerce (eJI) in detail, it should be underscored that the rules and the stakeholders' positioning are very much reflected in the WTO context as well, and in this way FTAs can be well perceived as active regulatory laboratories.[206] A second trend that can be observed 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 fairly binding deal with the EU (including an adequacy decision with regard to the essentially equivalent level of personal data protection), while also entering into liberal and ambitious digital trade commitments under DEAs and the CPTPP.

[41] As this article showed, Switzerland has not been a part of these developments and has not proactively engaged in rulemaking in the area of digital trade, apart from the 2023 EFTA-Moldova FTA. This contrast is true with regard to the EU but also with regard to actors of comparative international standing, networks and regulatory capacity, such as notably Singapore and the UK. Despite the fact that Switzerland may have a natural preference for the multilateral path (it is part of eJI together with 89 other WTO Members but has not submitted a separate communication for the eJI negotiations) and is bound by trade negotiations along its EFTA partners, this delay in engagement on issues of digital trade appears somewhat odd. It does not reflect the economic priorities of Switzerland and fails to secure its digital sovereignty.[207] This is likely to change, as the Federal Council has clearly acknowledged the importance of digital trade and underscored the need to create an appropriate rule-framework for Switzerland.[208] More concretely, this is about to change as the EFTA has now a model chapter on electronic commerce that can be well implemented, as the FTA with Moldova shows, which effectively follows the EU template (in particular including data flows provisions but coupled with personal data protection rules and a right to regulate), and as the basic agreement with the UK is about to be renegotiated to address digital trade as well.[209] Singapore is also a partner with whom deeper data economy commit-

206 Burri (2023), supra note 13.

207 For Switzerland's efforts in this regard, see e.g. Swiss Federal Council, *Strategie Digitalaussenpolitik 2021–2024*, 4 November 2020.

208 Swiss Federal Council, Digitalisierung – Handlungsfelder der Wirtschaftspolitik: Bericht des Bundesrates vom 9. Dezember 2022 [hereinafter 2022 Federal Council Report on Digitization].

209 The UK has stated that with regard to digital trade, it would: Seek commitments that facilitate free and trusted cross-border data flows and prohibit unjustified data localisation providing certainty to businesses that they can enter and operate in markets without additional data storage costs; Maintain the UK's high standards for personal data protection to ensure public trust in the flow of data which promotes consumers' engagement and participation in digital trade; Seek commitments to facilitate more efficient and secure international trade through use of digital technologies, including through paperless trading, which will reduce administrative barriers and transaction costs for business; Ensure customs duties are not imposed on electronic transmissions which keeps down costs for businesses and consumers; Cooperate on evolving areas of trade such as emerging technologies, data innovation, and environmentally sustainable digital trade to help support business adapt to future challenges and avoid a patchwork of different national rules and regulations which make trade and e-commerce more difficult. See UK Department for Business and Trade, supra note 201.

ments in the form of DEA, can be entered into,[210] and existing agreements with suitable partners can be updated to address digital trade issues.[211]

[42] This article seeks to stress that there is some urgency attached to formulating a clear stance for Switzerland in this regard and making sure that these initiatives in the pipeline become reality. Sceptics may still wonder: why the rush? As a more general response, one can say that this may be critical for the Swiss economy: first, because Swiss enterprises are already highly digitized and have been particularly innovative in areas such as fintech. Second, Switzerland could use the opportunities that FTAs present to expand the market for digital trade for these enterprises, including small- and medium-sized ones, which are already in a very advantageous position to reap all the benefits that well-crafted digital trade rules offer to them. This could also expand the market of these companies beyond traditional partners, hence not only contributing to economic growth but also to resilience in an increasingly complex world. Furthermore, there is already some proof that digital trade commitments, especially if they contain more specific rules, have an effect on the development of the digital economy and data-driven innovation.[212] There is also a need to prevent ongoing digital fragmentation, which has an impact on the global economy but also on the possibilities for businesses in domestic economies to thrive, as digital policy compliance costs are substantial and multiply with heterogeneity.[213] Beyond the economy, crafting digital trade rules for Switzerland has implications for its societal interests and the protection of the citizenry – in particular with regard to privacy protection but also with regard to newer areas, such as platform and AI regulation. In this sense, the digital trade provisions become critical for Switzerland's digital sovereignty.[214] Geopolitically too, a more proactive and potentially innovative positioning of Switzerland could send the right signals and strengthen Switzerland's role as a global player with compelling regulatory capacity and forward-oriented agenda.

[43] Faced with the current situation, one can also view Switzerland's slow adaption as an opportunity. As the issues that fall in the domain of data governance include not only digital trade but also multiple domestic and regional regulatory frameworks of different nature, Switzerland can strive to achieve coherence across these domains. This includes for instance on the international scene the updated adequacy decision with the EU, the new transatlantic privacy framework but also domestic developments, such as the new Data Protection Act, initiatives to regulate platforms, fintech and AI. Digitization calls for regulators to look across sectors and have an integrated approach – the executive branch, as well as Swiss politicians and industry lobbies, must become aware of these critical interdependencies. Switzerland can attain this interoperability, having entered the debates at a point where both the technology and the policy discussions have become more mature. But it should do this within a reasonable period of time, as the agenda could have been already set by the US, Japan, Singapore and the EU, considering what is important for them, and Switzerland might shift into the position of a mere rule-taker without the key advantages of tailoring its own regulatory framework.

---

210 Indeed, negotiations with EFTA are ongoing: https://www.efta.int/free-trade/free-trade-agreements/singapore.

211 See 2022 Federal Council Report on Digitization, supra note 208.

212 See e.g. Jeongmeen Suh/Jaeyoun Roh, «The Effects of Digital Trade Policies on Digital Trade», *The World Economy* 46 (2023), 2383–2407. With regard to the EU, see e.g. Köhler-Suzuki, supra note 133.

213 See in this sense Evenett/Fritz, supra note 34. See also Simon J. Evenett/Johannes Fritz/Tommaso Giardini, «Deterring Digital Trade without Discrimination», *AJIL Unbound* 117 (2023), 104–109.

214 See Chander/Sun, supra note 10.

Mira Burri, Professor of International Economic and Internet Law, University of Lucerne. The support of the European Research Council under Consolidator Grant 101003216 is gratefully acknowledged.