

Trade and Technology: Rebooting Global Trade for the Digital Millennium

FOREWORD

Shifting Sands: Taking Stock of an Extraordinary Year

EDITORIAL

Gautami Govindrajan & Ayushi Singh, *Curb Your Enthusiasm: The WTO E-Commerce Negotiations and the Developing World*

ARTICLES

Mira Burri, *Digital Transformation: Heralding in a New Era for International Trade Law*

James J. Nedumpara, *Skirmishes over Digital Service Taxes: The Perils and Systemic Costs of Section 301 Actions*

Craig Atkinson & Nicolás Schubert, *Augmenting MSME Participation in Trade with Policy Digitalisation Efforts: Chile's Contribution to 'An Internet of Rules'*

Gabriele Gagliani, *Techno-Economic Governance in the 21st Century: Converging Models for WIPO and the WTO?*

Marta Soprana, *The Digital Economy Partnership Agreement (DEPA): Assessing the Significance of the New Trade Agreement on the Block*

Trade, Law *and* Development

Vol. 13, No. 1

2021

PATRON

Hon'ble Prof. Poonam Saxena

FACULTY-IN-CHARGE

Rosmy Joan

EDITORS-IN-CHIEF

Amogh Pareek

Gautami Govindrajan

EDITORS

Ayushi Singh
(SENIOR CONTENT)
Abhinav Srivastav
Suvam Kumar

Sabil Verma
(MANAGING)
Anjali Sasikumar

Abilash V.
(TECHNICAL)
Sukanya V.
Tania Gupta

ASSOCIATE EDITORS

Aastha Asthana
Nishant Sharma
Shlok Patwa

Malaika Shivalkar
Pranav Karwa

Neerali Nanda
Rashmi John
Swikruti Nayak

COPY EDITORS

Akshita Saxena
Jahnvi Srivastava
Ria Chaudhary

Ananya Awasthi
Maulik Khurana
Vidhi Damani

Anushka Mathur
Nidhi Lakhotia
Yashvi Hora

CONSULTING EDITORS

Ali Amerjee
Manu Sanan

Aman
Meghana Sharafudeen
Shashank P. Kumar

Dishi Bhomawat
Prateek Bhattacharya

BOARD OF ADVISORS

B. S. Chimni
Jagdish Bhagwati
Ricardo Ramírez Hernández

Daniel Magraw
M. Sornarajah
Vaughan Lowe

Glenn Wiser
Raj Bhal
W. Michael Reisman

Published by

The Registrar, National Law University, Jodhpur

ISSN : 0976-2329 | eISSN : 0975-3346

DIGITAL TRANSFORMATION: HERALDING IN A NEW ERA FOR INTERNATIONAL TRADE LAW

MIRA BURRI*

Digital technologies, taken as a broad category of technological inventions and applications, can be said to fall under the rare class of “disruptive technologies” that trigger profound societal transformations. This may demand changes in law and policy that go beyond incremental adjustment and necessitate a rethinking of existing approaches. It is the purpose of this article to explore the interfaces between digitally spurred transformations and how these have been reflected, or not, in global trade law frameworks. The article discusses the current regulatory framework for digital trade: first, by exploring the state of affairs under the auspices of the World Trade Organization (WTO) and second, by analysing the more deliberate regulatory responses to the digital challenge formulated in free trade agreements (FTAs). The article finally seeks to contextualise the existing legal framework and assess its adequacy for the contemporary data-driven economy.

TABLE OF CONTENTS

- I. INTRODUCTION
- II. THE DIGITAL DISRUPTION AND THE CENTRALITY OF DATA TO CONTEMPORARY ECONOMIES
- III. HOW HAS TRADE LAW REACTED TO THE DIGITAL TRANSFORMATION?
 - A. THE STATE OF WTO LAW WITH REGARD TO DIGITAL TRADE
 - B. DIGITAL TRADE RULES IN FTAs
 - 1. OVERVIEW
 - 2. THE CPTPP AND THE USMCA
 - 3. THE EU APPROACH TO DIGITAL TRADE
 - 4. THE DEPA
- IV. APPRAISAL OF THE CURRENT STATE OF DIGITAL TRADE GOVERNANCE AND OUTLOOK

* Professor of International Economic and Internet Law, University of Lucerne, Switzerland. The author can be contacted at [mira.burri\[at\]unilu.ch](mailto:mira.burri[at]unilu.ch).

I. INTRODUCTION

It has been wisely said that “[i]t cannot be helped, it is as it should be, that the law is behind the times.”¹ While this is a statement one can still subscribe to, technology and the law have had in practice a more complex, multi-directional relationship, as technological advances have prompted law’s adaptation, and as the legal environment has facilitated or hindered technological change in general and discrete developments in particular.² Law’s reactions to technological changes have been different. It has sometimes been the case that law has coped with new situations without deliberate adjustment by a simple subsumption under existing rules; other times, incremental adjustments through case-law or the legislature have been sufficient. Nevertheless, some technologies can be particularly disruptive³ and trigger radical changes in the economy with spill-over effects across multiple societal contexts. Digital technologies, taken as a broad category of technological inventions and applications, can be said to fall under this rare class of ‘disruptive technologies’ that trigger profound societal transformations. This may demand changes in law and policy that go beyond incremental adjustment and necessitate a rethinking of existing approaches. It is the purpose of this article to explore the interfaces between digitally spurred transformations and how these have been reflected, or not, in global trade law frameworks.

After a brief introduction to the implications of digitisation for trade and trade policy, the article turns to the current regulatory framework for digital trade: first, by exploring the state of affairs under the auspices of the WTO and second, by analysing the more deliberate regulatory responses to the digital challenge

¹ Oliver Wendell Holmes Jr., *Law and the Court*, Speech at the Harvard Law School Association of New York (Feb. 15, 1913).

² See, e.g., John Gerard Ruggie, *International Responses to Technology: Concepts and Trends*, 29(3) INT’L ORG. 557, 557–83 (1975); Thomas Cottier, *The Impact of New Technologies on Multilateral Trade Regulation and Governance: The New Global Technology Regime*, 72(2) CHI.-KENT L. REV. 415, 415–36 (1996); Colin B. Picker, *A View from 40,000 Feet: International Law and the Invisible Hand of Technology*, 23(1) CARDOZO L. REV. 149, 149–219 (2001); *REGULATING TECHNOLOGIES: LEGAL FUTURES, REGULATORY FRAMES AND TECHNOLOGICAL FIXES* (Roger Brownsword & Karen Yeung eds., 2008); Daniel Gervais, *The Regulation of Inchoate Technologies*, 47(3) HOUS. L. REV. 665, 665–705 (2010); Mira Burri & Thomas Cottier, *Introduction: Digital Technologies and International Trade Regulation*, in *TRADE GOVERNANCE IN THE DIGITAL AGE 1–14* (Mira Burri & Thomas Cottier eds., 2012).

³ James Manyika et al., *Disruptive Technologies: Advances that Will Transform Life, Business, and the Global Economy*, MCKINSEY GLOB. INST. 1 (May, 2013), https://www.mckinsey.com/~media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/disruptive%20technologies/mgi_disruptive_technologies_full_report_may2013.pdf [hereinafter Manyika et al. (2013)].

formulated in FTAs. The focus here is placed on distinct advanced models of digital trade regulation — those of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), the United States Mexico Canada Agreement (USMCA), the Digital Economy Partnership Agreement (DEPA), and the newer templates of the European Union (EU). The article finally seeks to contextualise and assess the impact of the existing legal framework and its adequacy for the contemporary data-driven economy, pointing also at some current deficiencies and problems down the road.

II. THE DIGITAL DISRUPTION AND THE CENTRALITY OF DATA TO CONTEMPORARY ECONOMIES

Several excellent studies in recent years have pointed to the disruptive character of digital technologies and heralded the onset of a “fourth industrial revolution”⁴, calling for adequate regulatory responses.⁵ Yet, such responses, in general and specifically, in the area of trade law and policy, may be difficult to elaborate, as digital technologies have multi-faceted effects, and their evolution is neither linear nor clearly predictable.⁶ Things are only going to get more complicated as digital technologies grow more intimately entwined with societies, which are complex and multi-directional in and of themselves. Benkler and others have demonstrated that in such a networked setting, innovation takes on a different form.⁷ Hence, regulators must learn to deal with unpredictability and think of a policy design that can adequately address it. Critical in designing regulatory adjustments is also the demand for balancing the benefits against the risks of technological advancements. This has become particularly evident in recent years with the increased value of data and the related new set of concerns in the area of privacy protection.

⁴ KLAUS SCHWAB, *THE FOURTH INDUSTRIAL REVOLUTION* (2017) [hereinafter SCHWAB]. Schwab makes the following distinctions: The “First Industrial Revolution” was characterised by the use of water and steam power to mechanise production. The “Second” employed electric power for mass production. The “Third” applied electronics and information technology to automate production. Now, a “Fourth” Industrial Revolution is building on the Third. It is characterised by a fusion of technologies that blurs the lines between the physical, digital, and biological spheres. Floridi uses the term of the “Fourth Revolution” (see LUCIANO FLORIDI, *THE FOURTH REVOLUTION: HOW THE INFOSPHERE IS RESHAPING HUMAN REALITY* (2014)); see also Manyika et al. (2013), *supra* note 3.

⁵ SCHWAB, *supra* note 4.

⁶ Yochai Benkler, *Growth-Oriented Law for the Networked Information Economy: Emphasizing Freedom to Operate over Power to Appropriate*, in *RULES FOR GROWTH: PROMOTING INNOVATION AND GROWTH THROUGH LEGAL REFORM* 314, 313–42 (Kauffman Taskforce on Law, Innovation and Growth ed., 2011) [hereinafter Benkler]; Richard S. Whitt, *A Deference to Protocol: Fashioning a Three-dimensional Public Policy Framework for the Internet Age*, 31(3) *CARDOZO ARTS & ENT. L. J.* 689, 717–29 (2013) [hereinafter Whitt].

⁷ Benkler, *supra* note 6.

Data is now commonly mentioned in the debates on economic growth and innovation.⁸ Evidently, data has become so essential to economic processes that it is said to be the “new oil”.⁹ While this is not entirely a valid statement,¹⁰ it illustrates the new value associated with data. Like other factors of production, such as natural resources and human capital, it appears increasingly the case that much of modern economic activity, innovation and growth cannot occur without data.¹¹ Many researchers show that data has enormous potential as a catalyst for more efficient business operations, highly innovative societal solutions, and ultimately better policy decisions.¹² The transformative potential does not apply only to digitally-driven businesses, but also refers to brick-and-mortar, physical ones. For instance, the information collected in manufacturing may be used to improve operations, anticipate risks and avoid accidents, while public administration can be made more efficient and citizen-oriented.¹³

The growing importance of data for the digital economy has one critical implication in terms of trade and trade policies and that is that data *must flow* across

⁸ See, e.g., James Manyika et al., *Big Data: The Next Frontier for Innovation, Competition, and Productivity*, MCKINSEY GLOB. INST. (June 2011), https://www.mckinsey.com/~media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/big%20data%20the%20next%20frontier%20for%20innovation/mgi_big_data_full_report.pdf [hereinafter Manyika et al. (2011)]; see also James Manyika et al., *Digital Globalization: The New Era of Global Flows*, MCKINSEY GLOB. INST. (Mar., 2016), <https://www.mckinsey.com/~media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx> [hereinafter Manyika et al. (2016)].

⁹ *The world's most valuable resource is no longer oil, but data*, THE ECONOMIST (May 6, 2017), <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>.

¹⁰ See, e.g., Jennifer Daskal, *The Un-territoriality of Data*, 125(2) YALE L. J. 326, 326–98 (2015); for a fully-fledged analysis, see Lauren Henry Scholz, *Big Data Is Not Big Oil: The Role of Analogy in the Law of New Technologies*, 86(4) TENN. L. REV. 863, 863–93 (2019).

¹¹ Manyika et al. (2011), *supra* note 8; Daniel Castro & Alan McQuinn, *Cross-border Data Flows Enable Growth in All Industries*, INFO. TECHN. & INNOVATION FOUND. (2015); Manyika et al. (2016), *supra* note 8.

¹² See, e.g., Manyika et al. (2011), *supra* note 8; VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, *BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK* 13 (2013); Nicolaus Henke et al., *The Age of Analytics: Competing in a Data-Driven World*, MCKINSEY GLOB. INST. (Dec., 2016), <https://www.mckinsey.com/~media/mckinsey/industries/public%20and%20social%20sector/our%20insights/the%20age%20of%20analytics%20competing%20in%20a%20data%20driven%20world/mgi-the-age-of-analytics-full-report.pdf>.

¹³ See, e.g., Manyika et al. (2011), *supra* note 8.

borders. Otherwise, many of the digital innovations and applications that we are very much used to in everyday life, such as the provision of digital products and services or cloud computing, would be seriously compromised.¹⁴ Artificial Intelligence (AI), as a promising new development, is also dependent on data inputs.¹⁵ This fundamental dependency puts pressure on trade policy and necessitates some solutions. Yet, these may be particularly hard to formulate, as the use of data and the affordances of Big Data analytics raise a number of thorny governance questions around sovereignty, the protection of privacy,¹⁶ national security, and other domestic values and interests. These tensions between domestic and global rules and between economic and non-economic interests are bound to grow as the pervasiveness of data increases.¹⁷ Finding functioning reconciliation mechanisms may again prove difficult since the variations in approaches across jurisdictions can be significant, as well exemplified by the diverging approaches of the United States of America (US) and the EU towards the protection of privacy,¹⁸ as discussed later in this article.

¹⁴ See Anupam Chander, *National Data Governance in a Global Economy*, UC DAVIS LEGAL STUD. RES. PAPER 495, 2 (2016); Anupam Chander, *AI and Trade*, in *BIG DATA AND GLOBAL TRADE LAW* 115–27 (Mira Burri ed., 2021).

¹⁵ Kristina Irion & Josephine Williams, *Prospective Policy Study on Artificial Intelligence and EU Trade Policy*, AMSTERDAM: INST. INFO. L. (2019), https://www.ivir.nl/publicaties/download/ivir_artificial-intelligence-and-eu-trade-policy.pdf [hereinafter Irion & Williams]; *Machine Learning: The Power and Promise of Computers that Learn by Example*, ROYAL SOC'Y (Apr., 2017), <https://royalsociety.org/~media/policy/projects/machine-learning/publications/machine-learning-report.pdf>.

¹⁶ See, e.g., Daniel J. Solove, *A Taxonomy of Privacy*, 154(3) U. PA. L. REV. 506, 477–560 (2006); Joel R. Reidenberg, *The Transparent Citizen*, 47(2) LOY. U. CHI. L. J. 437, 437–63 (2015); Colin J. Bennett & Robin M. Bayley, *Privacy Protection in the Era of “Big Data”: Regulatory Challenges and Social Assessments*, in *EXPLORING THE BOUNDARIES OF BIG DATA* 205–27 (Bart van der Sloot, et al. eds., 2016); Urs Gasser, *Recoding Privacy Law: Reflections on the Future Relationship among Law, Technology, and Privacy*, 130(2) HARV. L. REV. 61, 61–70 (2016); Mira Burri & Rahel Schär, *The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy*, 6(1) J. INFO. POL'Y 479, 479–511 (2016); Mira Burri, *Interfacing Privacy and Trade*, 53(1) CASE WEST. RES. J. INT'L L. 35, 35–88 (2021) [hereinafter Burri on Interfacing Privacy and Trade (2021)].

¹⁷ Burri on Interfacing Privacy and Trade (2021), *supra* note 16.

¹⁸ See Case C-362/14, Maximilian Schrems v. Data Protection Commissioner (Schrems I), 2015 ECLI:EU:C:2015:650 and the subsequent Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited, Maximilian Schrems (Schrems II), 2020 ECLI:EU:C:2020:559, both of which rendered the agreements for data transfer between the US and EU (Safe Harbor and Privacy Shield respectively) invalid on the grounds that there were not enough safeguards and remedies in the US for EU citizens' data. See also Paul M. Schwartz, *The EU-US Privacy Collision: A Turn to Institutions and Procedures*, 126(7) HARV. L. REV. 1996, 1966–2009 (2013); Paul M. Schwartz & Daniel J. Solove, *Reconciling*

The lack of solutions based on forms of international cooperation has prompted diverse unilateral reactions in the broader realm of data sovereignty. Some of these reactions have been linked to a new set of regulations that, in effect, stifle digital trade. Recent studies have attempted to map and evaluate data on these emerging digital trade barriers.¹⁹ Digital barriers that can be particularly intrusive are the so-called ‘data localisation measures’ that compel companies to conduct certain digital trade-related operations within a country’s domestic boundaries. Policies requiring data servers to be located within the country, or those requiring local content and entailing government procurement preferences, and technology standards that favour local digital enterprises are examples of these policies. Besides Russia, Turkey, and China, a number of other countries have introduced a wide range of these measures, particularly after the 2013 Snowden revelations.²⁰ Foreign businesses may face greater expenses and sub-optimal processes as a result of such policies, which effectively limit market access.²¹ While some of these regulations may be justified on the grounds of privacy protection or national security concerns, limiting this new kind of ‘digital protectionism’ should be a priority for policymakers.

III. HOW HAS TRADE LAW REACTED TO THE DIGITAL TRANSFORMATION?

Even though the disruptive changes of digitisation may call for a variety of governance adjustments of different kinds and depth, it should be underscored that digital trade has not developed in a rule-free space — there are existing rules at the international level that have been applicable throughout the different phases of digital transformations. At the heart of this legal framework lie the rules of the WTO’s multilateral forum, as the WTO regulates all trade. Over time, the WTO framework has been complemented by a significant and rising number of preferential bilateral and regional trade agreements. This article discusses these rules in turn and reveals their importance for the contemporary data-driven

Personal Information in the United States and European Union, 102(4) CALIF. L. REV. 877, 877–916 (2014).

¹⁹ See, e.g., Digital Trade in the US and Global Economies, Part 1, Inv. No. 332–531, USITC Pub. 4415 (July 2013); Digital Trade in the US and Global Economies, Part 2, Inv. No. 332–540, USITC Pub. 4485 (Aug. 2014); Rachel Fefer et al., *Digital Trade and US Trade Policy*, CONG. RES. SERV. REP. R44565, 2017. For a country survey, see Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64(3) EMORY L. J. 677, 677–739 (2015) [hereinafter Chander & Lê]. For a dynamic database, see *The Digital Trade Estimates Project*, EUROPEAN CTR. FOR INT’L POLITICAL ECON., <http://ecipe.org/dte/>.

²⁰ Chander & Lê, *supra* note 19.

²¹ For a more detailed study, see OECD, *Emerging Policy Issues: Localisation Barriers to Trade*, TAD/TC/WP(2014)17/FINAL (May 12, 2015).

economy, evaluating the adequacy of the formulated responses to the digital transformations.

A. The State of WTO Law with regard to Digital Trade

The WTO membership was early to recognise the implications of digitisation for trade by launching a Work Programme on E-commerce in 1998.²² This initiative aimed to examine and, if needed, adjust the rules in the domains of trade in services, trade in goods, intellectual property (IP) protection, and economic development. While the E-commerce Work Programme was ambitious and far-reaching in scope, for a variety of reasons, it has borne no fruit now after more than two decades since its launch. Indeed, WTO law, despite some adjustments through the 1998 Information Technology Agreement (ITA), its update in 2015, and the 1998 Fourth Protocol on Telecommunications Services, is still in a state that disregards the Internet as a global communication and trade platform, the embeddedness of the Internet in virtually all societies around the world, as well as the specific technological affordances of the digital medium.²³ Despite this lack of legal adaptation, WTO law is not irrelevant. As has been well documented, the WTO is founded on solid principles of non-discrimination that can address future technology advancements, possibly in a better way than tailor-made solutions. It should be highlighted in this context that WTO law frequently addresses challenges in a technologically neutral manner, such as with regard to the implementation of the core non-discrimination principles of most-favoured-nation (MFN) and national treatment (NT), with regard to standards, trade facilitation, subsidies, and government procurement.²⁴ Furthermore, the WTO has the benefit of a dispute settlement mechanism that can foster legal development and evolution.²⁵ Despite the current crisis of the WTO dispute settlement institution,²⁶ the approach of finding a solution through the WTO's judicial arm has worked

²² World Trade Organization, Work Programme on Electronic Commerce, WTO Doc. WT/L/274 (adopted Sept. 25, 1998).

²³ Mira Burri, *The International Economic Law Framework for Digital Trade*, 135(2) ZEITSCHRIFT FÜR SCHWEIZERISCHES RECHT 10, 10–72 (2015) [hereinafter Burri (2015)]; WORLD TRADE ORGANIZATION, WORLD TRADE REPORT 2018: THE FUTURE OF WORLD TRADE (2018), https://www.wto.org/english/res_e/publications_e/world_trade_report18_e.pdf.

²⁴ For a fully-fledged analysis, see Mira Burri & Thomas Cottier, *Trade Governance in the Digital Age* (2012).

²⁵ See, e.g., The WTO at Ten: The Contribution of the Dispute Settlement System (Giorgio Sacerdoti et al. eds., 2006).

²⁶ See, e.g., Joost Pauwelyn, *WTO Dispute Settlement Post 2019: What to Expect?*, 22(3) J. INT'L ECON. L. 297, 297–321(2019).

fairly successfully in the digital trade arena,²⁷ particularly in clarifying and advancing the WTO law and in settling some of the difficult issues upon which the 160+ WTO members could not reach a compromise, such as, for instance, the applicability of the General Agreement on Trade in Services (GATS), the likeness test and the general exception clauses.

Despite the utility of the WTO's dispute settlement, as seen in a number of Internet-related cases, such as *US — Gambling* and *China — Audiovisual Products*,²⁸ the lack of political consensus on substance could not be overcome. A number of important issues still remain unresolved and expose the disconnect between the existing WTO rules, in particular under the GATS, and digital trade practices on the ground. A good example in this context are the critical questions of whether entirely new digital offerings should be classified as goods or services (and thus whether the more binding General Agreement on Tariffs and Trade (GATT) or the GATS apply), and if categorised as services, under the scope of which subsector they would fall. For instance, online games which are a new type of content platform, might fall under the discrete categories of computer and related services, value-added telecommunications services, entertainment, or audiovisual services. This classification is not insignificant, as it implies distinct obligations for the WTO members, the divergence in commitments being particularly radical between the telecommunications and the media sectors.²⁹ The classification conundrum is just one of the several concerns raised in the framework of the 1998

²⁷ Many major GATS cases have had a substantial Internet-related element. See Panel Report, *United States — Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WTO Doc. WT/DS285/R (adopted Nov. 10, 2004) [hereinafter Panel Report, *US — Gambling*]; Appellate Body Report, *US — Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WTO Doc. WT/DS285/AB/R (adopted Apr. 7, 2005) [hereinafter Appellate Body Report, *US — Gambling*]; Panel Report, *China — Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, WTO Doc. WT/DS363/R (adopted Aug. 12, 2009) [hereinafter Panel Report, *China — Audiovisual Products*]; Appellate Body Report, *China — Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, WTO Doc. WT/DS363/AB/R (adopted Dec. 21, 2009) [hereinafter Appellate Body Report, *China — Audiovisual Products*]; Panel Report, *China — Certain Measures Affecting Electronic Payment Services*, WTO Doc. WT/DS413/R (adopted Aug. 31, 2012).

²⁸ Panel Report, *US — Gambling*, *supra* note 27; Appellate Body Report, *US — Gambling*, *supra* note 27; Panel Report, *China — Audiovisual Products*, *supra* note 27; Appellate Body Report, *China — Audiovisual Products*, *supra* note 27.

²⁹ ROLF H. WEBER & MIRA BURRI, CLASSIFICATION OF SERVICES IN THE DIGITAL ECONOMY (2012); Shin-yi Peng, *Renegotiate the WTO "Schedule of Commitments"?: Technological Development and Treaty Interpretation*, 45(2) CORNELL INT'L L. J. 403, 403–30 (2012); Ines Willemyns, *GATS Classification of Digital Services - Does 'the Cloud' Have a Silver Lining?*, 53(1) J. WORLD TRADE 59, 59–82 (2019).

WTO Work Programme on E-Commerce that are yet to be resolved.³⁰ For instance, there is still no agreement on a permanent moratorium on customs duties on electronic transmissions and their content — an issue that can be considered as the bare minimum required for advancing the digital trade agenda.³¹

Despite the recent reinvigoration of the E-Commerce Work Programme with the 2019 Joint Statement Initiative, which is a major effort to move towards new rules on digital trade uniting more than eighty WTO Members,³² the feasibility of an agreement that will cover all the pertinent issues that the data-driven economy has brought about, including rules on cross-border data flows, source code or non-discrimination of digital products, appears limited.³³ At the time of writing, the negotiation proposals reveal stark divergences between the WTO Members, and even outright opposition from several countries, such as India and South Africa. These, mostly developing countries, claim that a liberal digital trade regime with few or no restrictions on data flows will limit the prospects for local businesses, would not sufficiently reflect the inequalities of the data-driven economy and create opportunities for developing and least-developed countries to catch up.

In the last two decades, due to these failings of the multilateral trade forum, a lack of purposeful action, and a lack of consensus for a future-oriented digital trade deal, nations have changed forums and employed FTAs to address current and emerging digital trade issues. The following parts look at the solutions found in these preferential treaties, starting with a brief overview of the developments and then a deep dive on a few more recent and particularly far-reaching agreements that helps us get a sense of the evolving regulatory framework for digital trade.

B. *Digital Trade Rules in FTAs*

1. Overview

FTAs have shaped the regulatory environment for digital trade. Out of the 353 FTAs entered into between 2000 and 2020, 188 contain provisions relevant for

³⁰ Sacha Wunsch-Vincent & Arno Hold, *Towards Coherent Rules for Digital Trade: Building on Efforts in Multilateral versus Preferential Trade Negotiations*, in TRADE GOVERNANCE IN THE DIGITAL AGE 179–221 (Mira Burri & Thomas Cottier eds., 2012).

³¹ There have been several instances where the moratorium has been only temporarily extended, the most recent being for a period of two years following a decision taken in 2019.

³² World Trade Organization, Joint Statement on Electronic Commerce, WTO Doc. WT/L/1056 (Jan. 25, 2019).

³³ See, e.g., Mira Burri, *Towards a Treaty on Digital Trade*, 55(1) J. WORLD TRADE 77, 77–101 (2021) [hereinafter Burri on Digital Trade (2021)].

digital trade, 113 have specific e-commerce provisions, and eighty-three have dedicated e-commerce chapters.³⁴ Although the pertinent rules remain heterogeneous and differ as to the issues covered, from their overall level of commitments and bindingness, it is evident that the move towards more detailed and binding provisions on digital trade has intensified significantly over the past few years.³⁵ This regulatory push in the domain of digital trade can be explained by the increased importance of the issue over time, as well as by the proactive role played by the US, which has sought to implement its “Digital Agenda”³⁶ in more than a dozen agreements over the course of the past two decades. The template endorsed by the US has also diffused, in the sense that identical or similar rules have been adopted and can be found in a number of non-US FTAs.³⁷ This should not however be perceived in a way that all countries have clear and proactive digital trade stances. Indeed, many countries, even highly developed and industrialised ones, such as those members of the European Free Trade Area (EFTA),³⁸ are still in the process of elaborating distinct digital trade strategies.

When looking at a particular treaty, one can find norms relevant for digital trade in different sections of the treaty text. The most relevant aspects of digital trade governance can be found in: (i) the specifically dedicated e-commerce FTA chapters; (ii) the chapters on cross-border supply of services (in particular in the telecommunications, computer and related, audio-visual, and financial services sectors); as well as in (iii) the chapters on IP protection.³⁹ The focus of this article is on the e-commerce chapters, which have been the main source of new

³⁴ This analysis is based on a dataset of all data-relevant norms in trade agreements (TAPED). See TAPED, UNIV. OF LUCERNE, <https://unilu.ch/taped>; see also Mira Burri & Rodrigo Polanco, *Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset*, 23(1) J. INT'L ECON. L. 187, 187–220 (2020) [hereinafter Burri & Polanco].

³⁵ Presently, digital trade provisions are, on average, included in more than 61% of all PTAs that were concluded in the said period, with an average of 1476 words found in e-commerce chapters and side agreements in the last five years. See Burri & Polanco, *supra* note 34; see also Ines Willems, *Agreement Forthcoming? A Comparison of EU, US, and Chinese RTAs in Times of Plurilateral E-Commerce Negotiations*, 23(1) J. INT'L ECON. L. 221, 221–44 (2020).

³⁶ Bipartisan Trade Promotion Authority Act, 19 U.S.C. (2001); Sacha Wunsch-Vincent, *The Digital Trade Agenda of the U.S.: Parallel Tracks of Bilateral, Regional and Multilateral Liberalization*, 58(1) AUSSENWIRTSCHAFT 7, 7–46 (2003); see also Henry Gao, *Regulation of Digital Trade in US Free Trade Agreements: From Trade Regulation to Digital Regulation*, 45(1) LEGAL ISSUES OF ECON. INTEGRATION 47, 47–70 (2018).

³⁷ See e.g., Manfred Elsig & Sebastian Klotz, *Data Flow-Related Provisions in Preferential Trade Agreements: Trends and Patterns of Diffusion*, in *BIG DATA AND GLOBAL TRADE LAW* 42–62 (Mira Burri ed., 2021).

³⁸ The EFTA members are Iceland, Liechtenstein, Norway and Switzerland.

³⁹ For analysis of all relevant chapters, see Burri (2015), *supra* note 23.

rulemaking. The e-commerce chapters play a dual role in the landscape of trade rules in the digital era. On one hand, they represent an attempt to compensate for the lack of progress in WTO law and remedy some of the ensuing uncertainties. On the other hand, the e-commerce chapters also include rules that have not been discussed in the context of the WTO negotiations. They seek the promotion and facilitation of e-commerce by addressing, for instance, e-contracts and paperless trading, as well as tackle the emergent regulatory dilemmas about cross-border data flows, new digital trade barriers and other novel issues, which can encompass questions ranging from cybersecurity to open government data. With regard to facilitation of digital trade, the number of FTAs that contain such rules is substantial, while only few agreements have rules on the newer set of issues and data in particular.⁴⁰ In the latter context, the CPTPP and the USMCA created important models as reviewed in the next part.

2. The CPTPP and the USMCA

The CPTPP was agreed upon in 2017 among eleven countries in the Pacific Rim,⁴¹ and entered into force on December 30, 2018. Despite the US having dropped out of the agreement with the start of the Trump administration, the CPTPP e-commerce chapter reflects the US efforts to secure obligations on digital trade and is a verbatim reiteration of the e-commerce chapter under the negotiated Trans-Pacific Partnership Agreement (TPP). Not unusually for US-led and other FTAs, the first part of the CPTPP e-commerce chapter clarifies that it applies “to measures adopted or maintained by a Party that affect[s] trade by electronic means”⁴² but excludes from this broad scope: (i) government procurement; and (ii) information held or processed by or on behalf of a Party, or measures related to such information, including measures related to its collection.⁴³ For greater certainty, measures affecting the supply of a service delivered or performed electronically are subject to the obligations set forth in the applicable provisions on investment and services;⁴⁴ however, some additional exceptions are also specified.⁴⁵ The following provisions address, again as customarily, some of the leftovers of the 1998 WTO E-commerce Programme and provide for the facilitation of online commerce. In this sense, Article 14.3 of the CPTPP bans the imposition of

⁴⁰ See e.g., Mira Burri, *Data Flows and Global Trade Law*, in *BIG DATA AND GLOBAL TRADE LAW* 11–41 (Mira Burri ed., 2021).

⁴¹ Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, and Vietnam.

⁴² Comprehensive and Progressive Agreement for Trans-Pacific Partnership, Dec. 30, 2018 [hereinafter CPTPP].

⁴³ *Id.*, art. 14.2(3).

⁴⁴ *Id.*, art. 14.2(4).

⁴⁵ *Id.*, arts. 14.2(5) & 14.2(6).

customs duties on electronic transmissions, including content transmitted electronically, and Article 14.4 of the CPTPP endorses the non-discriminatory treatment of digital products,⁴⁶ which are defined broadly pursuant to Article 14.1.⁴⁷ Article 14.5 of the 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 of 1996 and the United Nations (UN) Convention on the Use of Electronic Communications in International Contracts. Parties must endeavour to: (i) avoid any unnecessary regulatory burden on electronic transactions; and (ii) facilitate input by interested persons in the development of its legal framework for electronic transactions.⁴⁸ The provisions on paperless trading, electronic authentication, and electronic signatures complement this by securing equivalence of electronic and physical forms. In matters of paperless trading, it is explained that parties shall strive to make trade administration documents available to the public in digital form and treat documents submitted digitally as the legal equivalent of the paper version.⁴⁹ The provision on electronic signatures is more binding, stating that parties shall not deny the legal validity of a signature solely because the signature is in electronic form,⁵⁰ 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.⁵¹

The remainder of the provisions found in the CPTPP e-commerce chapter can be said to belong to the category of rulemaking that is more recent as well as more innovative and tackles the emergent issues of the data economy. Above all, the CPTPP expressly intends to prohibit the use of data localisation measures. Article

⁴⁶ 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. *Id.*, art. 14.2(3).

⁴⁷ A 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 digitised 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 categorised as trade in services or trade in goods.

⁴⁸ CPTPP, *supra* note 42, art. 14.5(2).

⁴⁹ *Id.*, art. 14.9.

⁵⁰ *Id.*, art. 14.6(1).

⁵¹ *Id.*, art. 14.6(2).

14.13(2) forbids parties from requiring a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory. The soft language from US–South Korea FTA on free data flows is also now framed as a hard rule: “[e]ach Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person”,⁵² so the commitment to a liberal data economy is quite clear.

Measures restricting digital flows or implementing localisation 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.”⁵³ These non-discriminatory conditions are similar to the strict test formulated by the general exception clauses of Article XIV of the GATS and Article XX of the GATT 1994 — a test that has been designed to balance trade and non-trade interests by excusing certain violations but is also extremely hard to pass, as the WTO jurisprudence up to the present date has shown.⁵⁴ It is noteworthy that the CPTPP test differs from the WTO rules in one significant way: whereas the GATT and GATS contain an exhaustive list of public policy objectives that may justify a WTO law violation, the CPTPP does not. Instead, it simply refers to the broad and open category of “legitimate public policy objective”.⁵⁵ This allows the CPTPP signatories to exercise more regulatory autonomy; yet, it may lead to legal uncertainty and remains to be tested in actual cases. It is also worth noting that the ban on localisation measures is somewhat softer with regard to financial services and institutions,⁵⁶ and government procurement has been entirely excluded from the scope of this obligation.⁵⁷

Next to the pertinent issue of cross-border data flows, the CPTPP addresses some other novel matters as well — one of them is software source code. Pursuant to Article 14.17, a CPTPP Member shall not require the transfer of, or access to, the

⁵² *Id.*, art. 14.11(2).

⁵³ *Id.*, art. 14.11(3).

⁵⁴ See, e.g., Henrik Andersen, Protection of Non-Trade Values in WTO Appellate Body Jurisprudence: Exceptions, Economic Arguments, and Eluding Questions, 18(2) J. INT'L ECON. L. 383, 383–405 (2015).

⁵⁵ CPTPP, *supra* note 42, art. 14.11(3).

⁵⁶ *Id.*, art. 14.1, the definition of “a covered person”, which excludes a “financial institution” and a “cross-border financial service supplier”. 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.

⁵⁷ *Id.*, art. 14.8(3).

source code of a 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.⁵⁸ This provision intends to safeguard software companies and addresses their concerns about potential losses of property rights in the form of patent, copyright or trade secrets, or security breaches in their proprietary code. It may also be viewed as a response to China's demands to access to source code from software producers selling in its market.

Article 14.8(2) provides for certain levels of data protection and mandates that every CPTPP party adopt or maintain a legal framework that provides for the protection of the personal information of the users of e-commerce. However, barring a general requirement that CPTPP parties must take into account the principles or guidelines of relevant international bodies, there are no criteria or specific benchmarks that the domestic legal framework on personal data protection must comply with.⁵⁹ Parties are also encouraged to make their data protection regimes more compatible by recognising lower levels of protection as equivalent.⁶⁰ The goal of these norms can be interpreted as a prioritisation of trade over privacy rights and can be problematic for countries sharing a different understanding of personal data protection, such as notably the European Union. The CPTPP also includes provisions on consumer protection,⁶¹ spam control,⁶² and net neutrality.⁶³ However, these are of soft legal nature. The same is true for the newly introduced rules on cybersecurity.⁶⁴

After the withdrawal of the US from the CPTPP, there was some uncertainty as to the direction the US will follow on matters of digital trade. The renegotiated North American Free Trade Agreement (NAFTA), now referred to as the USMCA, casts these doubts aside. The USMCA contains a comprehensive e-commerce chapter, which has now been properly titled as "Digital Trade" and follows all critical lines of the CPTPP; creating an even more ambitious template. With regard to

⁵⁸ The prohibition applies only to mass-market software or products containing such software. This means that tailor-made products, as well as the software used for critical infrastructure and those in commercially negotiated contracts, are excluded.

⁵⁹ CPTPP, *supra* note 42, art. 14.8(2). Footnote (6) 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."

⁶⁰ *Id.*, art. 14.8(5).

⁶¹ *Id.*, art. 14.17.

⁶² *Id.*, art. 14.14.

⁶³ *Id.*, art. 14.10.

⁶⁴ *Id.*, art. 14.16.

replicating the CPTPP model, the USMCA follows the same broad scope of application,⁶⁵ bans customs duties on electronic transmissions,⁶⁶ and binds the parties for non-discriminatory treatment of digital products.⁶⁷ Furthermore, the USMCA provides for a domestic regulatory framework that facilitates online trade by enabling electronic contracts,⁶⁸ electronic authentication and signatures,⁶⁹ and paperless trading.⁷⁰

The USMCA digital trade chapter sticks to the CPTPP model with regard to data issues as well, by ensuring a liberal environment through an explicit ban on data localisation⁷¹ and a binding rule on free information flows.⁷² Article 19.11 of the USMCA specifies further that parties can adopt or maintain a measure inconsistent with the free flow of data provision, if this is necessary to achieve a legitimate public policy objective, provided that there is no arbitrary or unjustifiable discrimination nor a disguised restriction on trade and the restrictions on transfers of information are not greater than necessary to achieve the objective.⁷³ Beyond these similarities with the CPTPP template, the USMCA introduces some novelties. The first one is that the USMCA departs from the standard US approach on very low data protection obligations and signals a slight shift by including a commitment to the guidelines of relevant international bodies.⁷⁴ Specifically mentioned in this regard are the APEC Privacy Framework and the updated Organization for Economic Co-operation Development (OECD) Guidelines on

⁶⁵ United States-Mexico-Canada Agreement art. 19.2, Sept. 30, 2018 (H.R./5430) (2019) [hereinafter USMCA].

⁶⁶ *Id.*, art. 19.3.

⁶⁷ *Id.*, art. 19.4.

⁶⁸ *Id.*, art. 19.5.

⁶⁹ *Id.*, art. 19.6.

⁷⁰ *Id.*, art. 19.9.

⁷¹ *Id.*, art. 19.12.

⁷² *Id.*, art. 19.11.

⁷³ *Id.*, art. 19.11(2). There is a footnote attached, which clarifies: “A measure does not meet the conditions of this paragraph if it accords different treatment to data transfers solely on the basis that they are cross-border in a manner that modifies the conditions of competition to the detriment of service suppliers of another Party.” The footnote does not appear in the CPTPP treaty text.

⁷⁴ *Id.*, art. 19.8(2). It requires the parties to:

[a]dopt 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).

Privacy and Transborder Flows of Personal Data.⁷⁵ The USMCA parties also acknowledge key data protection principles, which include: limitation on the collection, choice, data quality, purpose specification, use limitation, security safeguards, transparency, individual participation, and accountability,⁷⁶ and aim to provide remedies for any violations.⁷⁷ This is the first and only time so far that the US explicitly mentions such data principles in its treaties.

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”⁷⁸ and has become part of the prohibition on requirements for the transfer or access to software source code in Article 19.16 of the USMCA. The second refers to the recognition of “interactive computer services”⁷⁹ as particularly vital to the growth of digital trade and the newly inserted obligation to limit their liability. Parties pledge in this context not to:

[a]dopt or maintain measures that treat a supplier or user of an interactive computer service as an information content provider in determining liability for harms related to information stored, processed, transmitted, distributed, or made available by the service, except to the extent the supplier or user has, in whole or in part, created, or developed the information.⁸⁰

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.⁸¹ It also secures the application of Section 230 of the US Communications Decency Act,⁸² which insulates platforms from liability but has

⁷⁵ *Id.*

⁷⁶ *Id.*, art. 19.8(3).

⁷⁷ *Id.*, art. 19.8(4) & art. 19.8(5).

⁷⁸ *Id.*, art. 19.1.

⁷⁹ *Id.*, art. 19.17.

⁸⁰ *Id.*, art. 19.17(2). Annex 19-A creates specific rules with the regard to the application of art. 19.17 for Mexico, in essence postponing its implementation for three years.

⁸¹ On intermediaries’ liability, see, e.g., Sonia K. Katyal, *Filtering, Piracy, Surveillance and Disobedience*, 32(4) COLUM. J. L. & ARTS 401, 401–26 (2009); GOVERNANCE OF ONLINE INTERMEDIARIES: OBSERVATIONS FROM A SERIES OF NATIONAL CASE STUDIES (Urs Gasser & Wolfgang Schulz eds., 2015).

⁸² Communication Decency Act, 47 U.S.C. §230 (1996). It 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.”

been recently under attack in many jurisdictions in the face of fake news and other negative developments related to platforms' power in the digital space.⁸³

The third and rather liberal commitment of the USMCA parties concerns open and accessible government data. This is truly innovative and can be very relevant in the domain of designing domestic regimes for data governance. In Article 19.18 of the USMCA, the parties recognise that facilitating public access to and use of government information fosters economic and social development, competitiveness, and innovation. If a party decides 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.⁸⁴ There is, in addition, an endeavour to cooperate so as to expand access to and use of government information, including data, which the party has made public, for enhancing and generating business opportunities, especially for small and medium-sized enterprises (SMEs).⁸⁵

The US approach towards digital trade issues has also been confirmed by the recent US–Japan Digital Trade Agreement (DTA), signed on October 7, 2019, alongside the US–Japan Trade Agreement.⁸⁶ The US–Japan DTA, which has been the first dedicated digital trade agreement, can be said to replicate almost all provisions of the USMCA and the CPTPP,⁸⁷ including the new USMCA rules on open government data,⁸⁸ source code,⁸⁹ and interactive computer services,⁹⁰ but notably covering also financial and insurance services as part of the scope of agreement, which substantially extends its reach. Overall, the CPTPP/USMCA

⁸³ See, e.g., Lauren Feiner, *Big Tech's favourite law is under fire*, CNBC (Feb. 19, 2020) <https://www.cnbc.com/2020/02/19/what-is-section-230-and-why-do-some-people-want-to-change-it.html>. For an analysis of the free speech implications of digital platforms; see Jack M. Balkin, *Free Speech Is a Triangle*, 118(7) COLUM. L. REV. 2011, 2011–56 (2018).

⁸⁴ USMCA, *supra* note 65, art. 19.18(2).

⁸⁵ *Id.*, art. 19.8(3).

⁸⁶ Agreement between the United States of America and Japan concerning Digital Trade, Oct. 7, 2019.

⁸⁷ *Id.*, art. 7. Customs Duties; art. 8: Non-Discriminatory Treatment of Digital Products; art. 9: Domestic Electronic Transactions Framework; art. 10: Electronic Authentication and Electronic Signatures; Article 14: Online Consumer Protection; art. 11: Cross-Border Transfer of Information; art. 12: Location of Computing Facilities; art. 16: Unsolicited Commercial Electronic Messages; art. 19: Cybersecurity.

⁸⁸ *Id.*, art. 20.

⁸⁹ *Id.*, art. 17.

⁹⁰ *Id.*, art. 18. A side letter recognises the differences between the US and Japan's systems governing the liability of interactive computer services suppliers, and parties agree that Japan need not change its existing legal system to comply with art. 18.

template creates a distinct model for addressing the pertinent issues of data-driven economy, which has been followed by a great number of subsequent FTAs and its impact has been so augmented.⁹¹

3. The EU approach to Digital Trade

The EU approach to digital trade has not been as ambitious or as coherent as that of the US. It has also substantially developed over time in terms of the issues covered and the level of the binding commitments. Although, the agreement with Chile, which was signed in 2002, was the first to incorporate significant e-commerce provisions, the language was still cautious and confined to soft cooperation pledges in the services chapter;⁹² and in the fields of information technology, information society and telecommunications.⁹³ In more recent agreements, such as the EU–South Korea FTA (signed in 2009), the language is more concrete and slightly more binding. It imitates some of the US template provisions and affirms the applicability of the WTO Agreements to e-commerce related matters, as well as commits to a permanent duty-free moratorium on electronic transmissions, however interpreting this more narrowly as to capture services only. The EU has also sought commitments from its FTA partners to comply with the international standards of data protection, since it is particularly concerned about data protection policies and more robust safeguards for privacy.⁹⁴ Co-operation on digital trade issues is also increasingly framed in more concrete terms. There are stronger provisions on digital trade facilitation too, including norms on mutual recognition of electronic signature certificates, coordination on Internet service providers' liability, consumer protection, and paperless trading.⁹⁵

The 2016 EU agreement with Canada – the Comprehensive Economic and Trade Agreement (CETA) went a step further. The CETA provisions cover commitments ensuring: (i) clarity, transparency and predictability in the parties'

⁹¹ See, e.g., the Chile-Uruguay Free Trade Agreement, Oct. 4, 2016; Agreement to Amend the Singapore-Australia Free Trade Agreement, Oct. 13, 2016; Argentina-Chile Free Trade Agreement, Nov. 2, 2017; Singapore-Sri Lanka Free Trade Agreement, Jan. 23, 2018; Australia-Peru Free Trade Agreement, Feb. 12, 2018; Brazil-Chile Free Trade Agreement, Nov. 21, 2018; Australia-Indonesia Free Trade Agreement, Mar. 4, 2019.

⁹² Chile-European Community Association Agreement, Nov. 18, 2002, art. 102. The agreement states that “[t]he inclusion of this provision in this Chapter is made without prejudice of the Chilean position on the question of whether or not electronic commerce should be considered as a supply of services.”

⁹³ *Id.*, art. 37.

⁹⁴ Free Trade Agreement between the European Union and its Member States, of the one part, and the Republic of Korea, of the other part, art. 7.48, May 14, 2011, L 127/6.

⁹⁵ *Id.*, art. 7.49.

domestic regulatory frameworks; (ii) interoperability, innovation and competition in facilitating electronic commerce; as well as (iii) facilitating the use of e-commerce by SMEs.⁹⁶ The EU has been successful in deepening the privacy commitments and the CETA includes a specific rule on trust and confidence in e-commerce, which obliges the parties to adopt or maintain laws, regulations or administrative measures for the protection of personal information of e-commerce users in accordance with the international data protection standards.⁹⁷ However, there are no deep commitments on digital trade, nor there are any rules on data flows.

Overall, the EU has been cautious about including data-related requirements in its FTAs. Only lately has the EU taken a step towards such rules, whereby parties have agreed to consider commitments related to cross-border flow of information. A clause like this can be found in the 2018 EU–Japan Economic Partnership Agreement,⁹⁸ and in the modernisation of the trade part of the EU–Mexico Global Agreement. In the latter two agreements, the parties agree to *reassess* the need for inclusion of provisions on the free flow of data into the treaty, within three years of the entry into force of the treaty. This marked a slight but important shift in the EU’s policy on data flows, which is now fully endorsed in the EU’s currently negotiated deals with Australia,⁹⁹ New Zealand,¹⁰⁰ and Tunisia,¹⁰¹ which include in their draft digital trade chapters norms on the free flow of data as well as data localisation bans. This repositioning and newer commitments are, however, also linked with high levels of data protection.¹⁰²

⁹⁶ Comprehensive Economic and Trade Agreement, Canada-EU, art. 16.5, Oct. 30, 2016, O.J. (L 11) 23.

⁹⁷ *Id.*, art. 16.4.

⁹⁸ Agreement between the European Union and Japan for an Economic Partnership, art. 8.81, Dec. 27, 2018, O.J. (L 330).

⁹⁹ EU Proposal, EU-Australia Free Trade Agreement: Digital Trade, European Comm’n (2018), https://trade.ec.europa.eu/doclib/docs/2018/december/tradoc_157570.pdf.

¹⁰⁰ EU Proposal, EU-New Zealand Free Trade Agreement: Digital Trade, European Comm’n (2018), https://trade.ec.europa.eu/doclib/docs/2018/december/tradoc_157581.pdf.

¹⁰¹ EU PROPOSAL, EU-TUNISIA FREE TRADE AGREEMENT: DIGITAL TRADE, EUROPEAN COMM’N (2018), https://trade.ec.europa.eu/doclib/docs/2019/january/tradoc_157660.%20ALECA%202019%20-%20texte%20commerce%20numerique.pdf.

¹⁰² See Horizontal Provisions for Cross-Border Data Flows and for Personal Data Protection in EU Trade and Investment Agreements, EUROPEAN COMM’N (Feb. 2018), https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf.

The EU is willing to allow data flows only if coupled with the stringent and high data protection standards of its General Data Protection Regulation (GDPR).¹⁰³ The EU follows a specific model of endorsing and protecting privacy as a fundamental right in its currently negotiated trade deals, as well as in its proposal for WTO rules on electronic commerce.¹⁰⁴ On the one hand, the EU and its partners want to enforce a ban on data localisation measures and subscribe to a free data flow; on the other hand, these commitments are conditional: they are strongly affected by a dedicated article on data protection, which clearly states that: “[e]ach 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”(emphasis added).¹⁰⁵ This is followed by a paragraph that essentially endorses data sovereignty, particularly in the area of personal data protection:

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.¹⁰⁶

The EU also seeks to preserve the right to see how the implementation of the FTA rules concerning data flows impacts the conditions of privacy protection, so there is a possibility of review within three years of the entry into the agreement if parties are open to review the list of restrictions as they please.¹⁰⁷ In addition, there is a broad carve-out, in the sense that:

¹⁰³ 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.

¹⁰⁴ World Trade Organization, Joint Statement on Electronic Commerce, EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce, WTO Doc. INF/ECOM/22 (2019).

¹⁰⁵ See, e.g., draft Australia-European Union Free Trade Agreement, art. 6(1), June 18, 2018 (emphasis added). The same wording is found in the draft EU-New Zealand and the EU-Tunisia FTAs.

¹⁰⁶ See, e.g., *id.*, art. 6(2). The same wording is found in the draft EU-New Zealand and the EU-Tunisia FTAs.

¹⁰⁷ See, e.g., *id.*, art. 5(2). The same wording is found in the draft EU-New Zealand and the EU-Tunisia FTAs.

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.¹⁰⁸

As a result, the EU retains plenty of regulatory leeway for its current and future data protection measures, or indeed any measure that may affect objectives and interests that are important to the EU and its twenty-seven member states. The exception is also fundamentally different 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.¹⁰⁹

While the new EU approach has been confirmed by the recently adopted post-Brexit Trade and Cooperation Agreement (TCA) with the United Kingdom,¹¹⁰ which contains a comprehensive digital trade title with data-related provisions, rules on software source code and open government data,¹¹¹ the EU also appears likely to tailor its template depending on the trade partner. The currently negotiated modernisation of the agreement with Chile lacks a provision on data flows and data protection,¹¹² and includes merely a place-holder for rules on data flows.¹¹³ The recently signed agreement with Vietnam, which entered into force on August 1, 2020, has only a few co-operation provisions on e-commerce as part of the services chapter and no mention of either data or privacy protection is made.¹¹⁴

4. The DEPA

¹⁰⁸ See, e.g., *id.*, art. 2. The same wording is found in the draft EU-New Zealand and the EU-Tunisia FTAs.

¹⁰⁹ Svetlana Yakovleva, Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy, 74(2) U. MIAMI L. REV. 416, 496 (2020).

¹¹⁰ Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part, Dec. 31, 2021, O. J. L 149/10 [hereinafter TCA].

¹¹¹ See *id.*, Title III: Digital Trade, art. 196–212.

¹¹² EU proposal, EU-Chile Free Trade Agreement: Title on Digital Trade, European Comm'n, https://trade.ec.europa.eu/doclib/docs/2018/february/tradoc_156582.pdf.

¹¹³ EU proposal, EU-Indonesia Free Trade Agreement: Title on Digital Trade, European Comm'n, https://trade.ec.europa.eu/doclib/docs/2017/september/tradoc_156106.pdf.

¹¹⁴ Free Trade Agreement between European Union and The Socialist Republic of Vietnam, 2018 O.J. (L 186), <http://trade.ec.europa.eu/doclib/press/index.cfm?id=1437>.

Beyond different approaches to digital trade as a topic of trade negotiations and deals, more recently, states have realised that enhanced co-operation is needed and possible outside of trade venues. The 2020 DEPA between Chile, New Zealand, and Singapore,¹¹⁵ all parties also to the CPTPP, is an expression of this. The DEPA is not conceptualised purely as a trade agreement but one that seeks to address the broader issues of the digital economy. In this sense, its scope is broad and flexible, and covers several emergent issues, such as AI and digital inclusion. The agreement is also not a closed deal but one that is open to other countries,¹¹⁶ and the DEPA is meant to complement the WTO negotiations on e-commerce and build upon the digital economy work underway within the Asian-Pacific Economic Cooperation (APEC), the OECD and other international forums. To enable flexibility and cover a wide range of issues, the DEPA follows a modular approach. 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 operationalisation 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 with regard to amendments, entry into force, accession and withdrawal (Module 16).

The type of rules varies across the different modules. On the one hand, all rules of the CPTPP are replicated, some of the USMCA rules, such as the one on open government data¹¹⁷ (but not source code), and some of the US–Japan DTA provisions, such as the one on information and communications technology (ICT) goods using cryptography,¹¹⁸ have been included too. On the other hand, there are many other provisions, so far unknown to trade agreements. Some of these rules try to facilitate the functioning of the digital economy and enhance co-operation on key issues. For instance, Module 2 on business and trade facilitation includes next to the standard CPTPP-like norms,¹¹⁹ additional efforts “to establish or maintain a seamless, trusted, high-availability and secure interconnection of each

¹¹⁵ Digital Economy Partnership Agreement between Singapore, Chile and New Zealand, June 11, 2020 [hereinafter DEPA].

¹¹⁶ *Id.*, art. 16.2

¹¹⁷ *Id.*, art. 9.4.

¹¹⁸ *Id.*, art. 3.4. The article also provides detailed definitions of cryptography, encryption, and cryptographic algorithm and cipher.

¹¹⁹ *Id.*, art. 2.2 & art. 2.3. Art. 2.2: Paperless Trading; Art. 2.3: Domestic Electronic Transactions Framework.

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."¹²⁰ Parties have also touched upon other important issues around digital trade facilitation, such as electronic invoicing (Article 2.5), express shipments and clearance times (Article 2.6), logistics (Article 2.4) and electronic payments (Article 2.7). Module 8 on emerging trends and technologies is also particularly interesting to mention, as it highlights a range of key topics that demand attention by policymakers, such as in the areas of financial technology (FinTech) and AI. In the latter domain, the parties agree to promote the adoption of ethical 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 recognised principles or guidelines, including explainability, transparency, fairness, and human-centred values.¹²¹ The DEPA parties also recognise the interfaces between the digital economy and government procurement and broader competition policy and agree to co-operate on these issues actively.¹²² Along this line of covering broader policy matters to create an enabling and trust-enhancing environment that is also not solely focused on and driven by economic interests, DEPA deals with the importance of a rich and accessible public domain¹²³ and digital inclusion, which can cover enhancing cultural and people to people links, including between Indigenous Peoples, and improving access for women, rural populations, and low socio-economic groups.¹²⁴

Overall, the DEPA is a unique and future-oriented project that covers well the broad range of issues that the digital economy impinges upon and offers a sound basis for harmonisation and interoperability of domestic frameworks and international co-operation that adequately takes into account the complex challenges of contemporary data governance that has essential trade but also non-trade elements.

IV. APPRAISAL OF THE CURRENT STATE OF DIGITAL TRADE GOVERNANCE AND OUTLOOK

The data-driven economy poses diverse and often hard to address challenges for policymakers in the regulation of digital trade. The conventional trade policy stance

¹²⁰ *Id.*, art. 2.2(5). "Single window" is defined as a facility that allows Parties involved in a trade transaction to electronically lodge data and documents with a single-entry point to fulfil all import, export and transit regulatory requirements (art. 2.1 DEPA).

¹²¹ *Id.*, art. 8.2(2) & art. 8.2(3).

¹²² *Id.*, art. 8.3 & art. 8.4.

¹²³ *Id.*, art. 9.2.

¹²⁴ *Id.*, art. 11.2.

of seeking reduced tariffs and further liberalisation of services sectors does not suffice, and there is a clear demand for enhanced regulatory co-operation that interfaces domestic regimes and provides for legal certainty. The multilateral forum of the WTO as the core of international economic law and an organisation with almost universal membership would be the optimal venue to address digital trade issues — both in the sense of older classification and services regulation issues and newer topics, such as data flows. Yet, so far and presumably in the near future, the WTO appears somewhat stuck and can deliver neither swift nor comprehensive solutions.¹²⁵ FTAs have served as valuable regulatory laboratories in the meantime that have, although in a patchwork manner, dealt with many of the pertinent issues and advanced a new regulatory model for digital trade. It contains a number of WTO-plus commitments and clarifies some issues the WTO members could not agree upon, such as the permanent duty-free regime for electronic transactions. More importantly, the FTAs tackle certain WTO-extra issues, such as consumer protection, privacy and safeguards for the free flow of data. The closer examination of the CPTPP and the USMCA showed the breadth of the topics covered, and the deep intervention of some of the agreed upon norms, such as those related to localisation bans and free cross-border data flows. The CPTPP/USMCA template is not however universally accepted — indeed, as mentioned earlier, only very few treaties have rules on data and many countries, such as the EU Member States, have chosen a much more cautious approach towards digital trade, which gives them policy space domestically and more opportunities to protect their citizens and their sovereignty.¹²⁶

The question of whether trade forums are at all the right ones to address the issues that the data-driven economy has raised is still also open,¹²⁷ as trade forums tend to *think* in terms of trade crossing borders through brick-and-mortar customs houses and incremental innovation through protected investments in production,¹²⁸ and are still very much top-down, state-centred and opaque rulemaking venues.¹²⁹ It should be highlighted in this context that while it is clear that digital technologies have had an impact on the economy as well as on social and cultural practices, they have also strongly affected the law and governance

¹²⁵ See, e.g., Burri on Digital Trade (2021), *supra* note 33.

¹²⁶ See, e.g., Burri on Interfacing Privacy and Trade (2021), *supra* note 16; see also Gregory Shaffer, *Trade Law in a Data-Driven Economy: The Need for Modesty and Resilience*, UC IRVINE LEGAL STUD. RES. PAPER SERIES NO. 2020–49 (2020) [hereinafter Shaffer].

¹²⁷ Shaffer, *supra* note 126; Mira Burri, The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation, 51 UC DAVIES L. REV. 65, 65–132 (2017).

¹²⁸ Thomas J. Bollyky & Petros C. Mavroidis, *Trade, Social Preferences, and Regulatory Cooperation: The New WTO-Think*, 20(1) J. INT'L ECON. L. 1, 1–30 (2017).

¹²⁹ See, e.g., Sungjoon Cho & Claire R. Kelly, *Are World Trading Rules Passé?*, 53 VAND. J. TRANSNAT'L L. 623, 623–66 (2013).

patterns in general. Governance models have become less state-centred, and there is a proliferation of regulatory forms that involve multiple stakeholders, with varied types of supervisory and controlling functions entrusted to the state.¹³⁰ Trade law venues need to take into account this evolution and become permeable to multi-stakeholder involvement framed within a more transparent framework, which may reduce the scepticism as to the appropriateness of trade forums and effectively tackle their deficiencies as to democratic participation and accountability. Analogies to Internet Governance processes may be particularly useful in this context.¹³¹ The recent discourse on AI technologies clearly demands such public engagement and seeks to endorse respect for human autonomy, prevention of harm, fairness and explicability.¹³² As data governance is intrinsically linked to the functioning of the Internet as an end-to-end generative platform,¹³³ it may also be important to consider, and where possible integrate, its underlying and complementary principles of Internet openness, security and privacy,¹³⁴ as well as to contemplate the use of middle-out approaches of governance that combine top-down and bottom-up regulation.¹³⁵ While the WTO has been so far unresponsive to such governance shifts, FTAs may offer suitable venues, with more open and flexible procedural frameworks and participatory and co-regulatory elements, as the DEPA discussed above suggests. Overall, regulatory co-operation is more likely to evolve through multiple channels, a process of learning and a combination of hard and soft law.¹³⁶

¹³⁰ See, e.g., Viktor Mayer-Schönberger, *The Shape of Governance: Analyzing the World of Internet Regulation*, 43 VA. J. INT'L L. 605, 605–73 (2003); Orly Lobel, *The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought*, 89(2) MINN. L. REV. 342, 342–470 (2004); CHRISTOPHER T. MARSDEN, *INTERNET CO-REGULATION: EUROPEAN LAW, REGULATORY GOVERNANCE AND LEGITIMACY IN CYBERSPACE* (2011); Michael Latzer et al., *Self- and co-Regulation: Evidence, Legitimacy and Governance Choice*, in *ROUTLEDGE HANDBOOK OF MEDIA LAW* 373–397 (Monroe Price & Stefaan Verhulst eds., 2012) [hereinafter Latzer et al.]; Ugo Pagallo et al., *The Middle-out Approach: Assessing Models of Legal Governance in Data Protection, Artificial Intelligence, and the Web of Data*, 7(1) THEORY & PRAC. LEGIS. 1, 1–25 (2019) [hereinafter Pagallo et al.].

¹³¹ See, e.g., Neha Mishra, *Building Bridges: International Trade Law, Internet Governance, and the Regulation of Data Flows*, 52(463) VAND. J. TRANSNAT'L L. 463, 463–509 (2019) [hereinafter Mishra].

¹³² See, e.g., Irion & Williams, *supra* note 15.

¹³³ See, e.g., Jonathan L. Zittrain, *The Future of the Internet – and How to Stop It* (2008); Whitt, *supra* note 6.

¹³⁴ Mishra, *supra* note 131.

¹³⁵ Latzer et al., *supra* note 130; Pagallo et al., *supra* note 130.

¹³⁶ Shaffer, *supra* note 126.