Summer, 2025
Vol. XVI, No. 2

Trade, Law *and* Development

ISSN: 0976 - 2329
eISSN: 0975 - 3346

TL&D

Trade, Law *and* Development

Vol. 16, No. 2 2025

Trade, Law *and* Development

Vol. 16, No. 2 2025

TABLE OF CONTENTS

ARTICLES, NOTES AND COMMENTS

Trade, Law *and* Development

Mira Burri, *Human Rights Implications of Digital Trade Law*
16(2) TRADE L. & DEV. 289 (2025)

HUMAN RIGHTS IMPLICATIONS OF DIGITAL TRADE LAW

MIRA BURRI*

Digital trade law has become one of the most dynamic fields of international law, as individual states and the global community have engaged in creating a new, albeit fragmented, rule-framework for the data-driven economy. This has unfolded almost exclusively through bilateral and regional trade agreements that regulate the digital economy by devising specific and at times far-reaching rules on non-discrimination of digital products, source code and cross-border data flows, to name but a few. Many of these economically driven provisions and the changes that they trigger in domestic regulatory regimes have serious human rights implications. Some of the tensions, in particular around personal data protection, have found reflection in policy and academic discussions. The implications for other human rights have been, however, often ignored. It is the article's objective to address this gap. First, by providing a detailed analysis of the current digital trade law framework, advanced through far-reaching treaties, such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), the United States-Mexico-Canada Agreement (USMCA) and the new generation of Digital Economy Agreements (DEAs). Second, by exploring the human rights implications of selected provisions in more detail, starting with the more conventional discussion of privacy and then freedom of speech, and moving towards the less explored interfaces with development. The article's overall enquiry seeks to feed into a more nuanced discussion of digital trade regulation and towards better interfacing of digital trade law with human rights.

TABLE OF CONTENTS

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

I. INTRODUCTION

Digital trade law has become one of the most dynamic fields of international law, as individual states and the global community realised the need to create a rule framework that regulates the data-driven economy in a manner that reflects its specificities and necessarily departs from the brick-and-mortar premise of the international trade regime. In this sense, the last decade has seen the adoption of a great number of treaties, particularly in the form of bilateral and regional Preferential Trade Agreements (PTAs), that regulate the digital economy by devising specific and at times far-reaching rules on non-discrimination of digital products, source code and cross-border data flows, to name but a few. Many of these economically driven provisions and the changes that they trigger in domestic regulatory regimes have serious human rights implications. On one hand, because they directly address some of the fundamental rights and freedoms and on the other hand, because they define the policy space that states have to protect these rights and freedoms at home. Some of these tensions have not gone unnoticed, and there is a vibrant discussion, both in policy and in academic circles, on the repercussions of digital trade regulation for personal data protection and the right to privacy. This article's objective is to cover these debates but also to look beyond them by exploring possible implications for other human rights. One important element of this analysis will also be to assess the policy space that treaty parties have in the digital domain and the available mechanisms to reconcile economic and non-economic concerns. This may be critical for identifying the avenues that states have domestically to navigate the regulatory landscape for digital trade while safeguarding the rights of their citizenry. Hopefully, the article's overall enquiry will feed into a more nuanced discussion of digital trade regulation and link to the rich literature on international economic law and human rights, that has yet to be updated to take the powerful impact of digitisation into account.

To advance this research agenda, the article begins with an overview of the

regulatory landscape for digital trade, followed by a deep dive into the most advanced treaty templates — a discussion that also helps the reader understand the positioning of the different stakeholders. The article's subsequent part explores the human rights implications of selected provisions in more detail, starting with the more conventional discussion of privacy and then freedom of speech, and moving towards the less explored interfaces with development. The article concludes with a summary of the presented enquiries and elaborates some recommendations.

II. THE DYNAMIC AND FLUID LANDSCAPE OF GLOBAL DIGITAL TRADE LAW

A. Introduction

As legal adaptation under the umbrella of the multilateral forum of the World Trade Organization (WTO) has stalled, and despite the current negotiations under the Joint Statement Initiative on Electronic Commerce (eJSI),[1] the regulatory environment for digital trade has been primarily shaped by PTAs. Out of the 465 agreements[2] signed between January 2000 and November 2024, 231 have provisions on e-commerce/digital trade, and 135 contain dedicated e-commerce/digital trade chapters.[3] Although the pertinent rules remain 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 markedly over the years, with a significant jump over the last five years.[4] This regulatory push in the domain of digital trade can be explained with the increased

---

[1] On the progress and more recent developments under the Joint Statement Initiative on Electronic Commerce (eJSI), *see*, *e.g.*, Mira Burri, *A WTO Agreement on Electronic Commerce: An Enquiry into its Substance and Viability*, 53 GEO. J. OF INT'L L. 565–625 (2023); Yusuf Ismail, *The Evolving Context and Dynamics of the WTO Joint Initiative on E-commerce: The Fifth-Year Stocktake and Prospects for 2023*, INT'L INST. FOR SUSTAINABLE DEV. & CUTS INT'L (2023), https://www.iisd.org/publications/report/wto-joint-initiative-e-commerce-fifth-year-stocktake; Rashmi Jose & Rashid S. Kaukab, *WTO Joint Initiative on E-Commerce State of Play: Past, Present, and Future* (2024), https://www.iisd.org/publications/report/wto-joint-initiative-e-commerce-state-of-play.

[2] The number of valid agreements is 428, accounting for agreements that have been discontinued or replaced.

[3] This analysis is based on a dataset of all digital trade relevant norms in trade agreements, i.e. Trade Agreements Provisions on Electronic Commerce and Data (TAPED). *See* Mira Burri & Rodrigo Polanco, *Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset*, 23 J. INT'L ECON. L. 187, 187–220 (2020); Mira Burri et al., *The Evolution of Digital Trade Law: Insights from TAPED*, 23 WORLD TRADE REV. 190, 190–207 (2024) [hereinafter Burri I]. For all data, as well as updates of the dataset, see Mira Burri, TAPED: A Dataset on Digital Trade Provisions, UNIVERSITY OF LUCERNE, https://unilu.ch/taped.

[4] *See*, *e.g.*, Burri I, *supra* note 3.

importance of the issue but also, at least in the early stages, with the proactive role played by the United States (U.S.),[5] as it forcefully endorsed its "Digital Agenda"[6] through the PTA channel. The diffusion of dedicated digital trade templates is not, however, limited to U.S. agreements, and several other PTAs, such as Singapore-Australia, Thailand-Australia, New Zealand-Singapore, Japan-Singapore, and South Korea-Singapore, contain comparable rules. The geopolitics of digital trade rulemaking have also changed over time, with the U.S. definitively retreating from its "rule-pusher" role in October 2023[7] and with Singapore now emerging as the leading legal entrepreneur, in particular with the new generation of DEAs.[8] Participation in both digital trade[9] and digital trade rulemaking is, however, still unevenly distributed. While, especially in recent years, one can observe increased diversity in the parties negotiating digital trade agreements, only 27 agreements with digital trade provisions include least developed countries (LDCs), and only 12 such agreements have been concluded among developing countries and LDCs.[10] Some

---

[5] *See* Manfred Elsig & Sebastian Klotz, *Data Flow-Related Provisions in Preferential Trade Agreements: Trends and Patterns of Diffusion*, *in* BIG DATA AND GLOBAL TRADE LAW 42–46 (Mira Burri ed., 2021).

[6] The "Digital Agenda" was part of the fast-track authority to conclude trade agreements with a simplified congressional ratification procedure introduced through the Bipartisan Trade Promotion Authority Act of 2002 § 19 U.S.C. § 2101(b)(2), 2102(b)(4), 2102(b)(7)(B), 2103(d), 2102(b)(9). The sections deal with services, intellectual property rights, IT products and e-commerce respectively. *See* Sacha Wunsch-Vincent, *The Digital Trade Agenda of the US*, 58 SWISS REV. INT'L ECON. REL. (AUSSENWIRTSCHAFT) 7–46 (2003); Henry Gao, *Regulation of Digital Trade in US Free Trade Agreements: From Trade Regulation to Digital Regulation*, 45 LEGAL ISSUES OF ECON. INTEGRATION 45, 47–70 (2018).

[7] As of 24 October 2023, the US has withdrawn its proposals on cross-border data flows, data localisation, and source code provisions from the WTO's eJSI Commerce and PTA negotiations. The United States Trade Representative (USTR) stated that, while the US remains active under the eJSI, it wished to evaluate these provisions that might "prejudice or hinder those domestic policy considerations". *See* Press Release, USTR Statement on WTO-E-Commerce Negotiations, United States Trade Representative (Oct. 24, 2023), https://ustr.gov/about-us/policy-offices/press-office/press-releases/2023/october/ustr-statement-wto-e-commerce-negotiations; Dan Dupont, *U.S. to End Support for WTO E-Commerce Proposals, Wants "Policy Space" for Digital Trade Rethink*, INSIDE U.S. TRADE (Oct. 24, 2023), https://insidetrade.com/daily-news/us-end-support-wto-e-commerce-proposals-wants-policy-space-digital-trade-rethink.

[8] Burri I, *supra* note 3.

[9] *See, e.g.,* Bhavya Agarwal & Neha Mishra, *Addressing the Global Data Divide through Digital Trade Law*, 14 TRADE L. & DEV. 238, 238–289 (2022) [hereinafter Agarwal & Mishra]; Mira Burri, *Inequalities in Digital Trade and Digital Trade Regulation*, *in* CONTESTED EQUALITY: INTERNATIONAL AND COMPARATIVE LEGAL PERSPECTIVES 203–220 (Elif Askin & Hanna Stoll eds., 2024) [hereinafter Burri II].

[10] Outliers are two agreements by Cambodia, which include dedicated e-commerce chapters. *See* Free Trade Agreement, China-Cambodia, Oct. 12, 2020,

regions, such as Africa and the Caribbean, are effectively not participating in the shaping of the digital trade law, at least thus far.

The relevant aspects of digital trade governance can be found in: (1) the specifically dedicated electronic commerce/digital trade PTA chapters; (2) the chapters on cross-border supply of services (with particular relevance of the telecommunications, computer and related, audiovisual and financial services sectors); as well as in (3) the chapters on intellectual property (IP) protection.[11] In this article, the focus is exclusively on the electronic commerce/digital trade chapters, as well as on the new type of "digital only" treaties — the DEAs — which have together become the source of new rulemaking in the area of digital trade, including far-reaching beyond the border effects.

The electronic commerce/digital trade chapters play a dual role in the landscape of trade rules in the digital era. On the one hand, they compensate for the lack of progress in the WTO and address many of the questions of the 1998 WTO Electronic Commerce Programme[12] that have been discussed but remained open.[13] For instance, a majority of the chapters recognise the applicability of WTO rules to electronic commerce[14] and establish an express and permanent duty-free moratorium on electronic transmissions.[15] In most of the templates tailored along the U.S. model, the chapters also include a clear definition of "digital products", which treats products delivered offline equally as those delivered online,[16] so that technological neutrality is ensured and some of the classification dilemmas of the General Agreement on Trade in Service (GATS) cast aside. The electronic commerce/digital trade chapters also include rules that have not been treated in the context of the WTO negotiations — the so-called "WTO-extra" issues. One can

---

https://fta.mofcom.gov.cn/cambodia/xieyi/xieyizw_en.pdf; Comprehensive Economic Partnership Agreement, U.A.E.-Cambodia, June 8, 2023, https://www.moec.gov.ae/documents/20121/1347101/UAE+Cambodia+CEPA+4+%282%29.pdf.

[11] For analysis of all relevant chapters, see Mira Burri, *The Regulation of Data Flows in Trade Agreements*, 48 GEO. J. INT'L L. 408, 408–448 (2017).

[12] WTO, WORK PROGRAMME ON ELECTRONIC COMMERCE, WT/L/274 (Sept. 30, 1998).

[13] SACHA WUNSCH-VINCENT, THE WTO, THE INTERNET AND DIGITAL PRODUCTS: EC AND US PERSPECTIVES (2006); Mira Burri, *The Impact of Digitization on Global Trade Law*, 24 GER. L. J. 551, 551–573 (2023); Burri I, *supra* note 3.

[14] *See*, *e.g.*, Free Trade Agreement, U.S.-Sing., art.14.3, 1, May 6, 2003, 117 Stat 948 [hereinafter U.S.-Singapore FTA]; Free Trade Agreement, U.S.-Austl., art. 16.1, May 18, 2004, 118 Stat 919 [hereinafter U.S.-Austl. FTA].

[15] *See*, *e.g.*, U.S.-Singapore FTA, *supra* note 14, art. 14.3; Free Trade Agreement, U.S.-Chile, June 6, 2003, art.15.3, 117 Stat 909.

[16] *See*, *e.g.*, U.S.-Singapore FTA, *supra* note 14, art. 14.3; U.S.-Austl. FTA, *supra* note 14, art. 16.4.

group these rules into two broader categories: (1) rules that target digital trade facilitation, such as paperless trading, electronic authentication, and electronic contracts; and (2) data governance rules that address cross-border data flows, data localisation measures and novel questions triggered by the implications of the data-driven economy.

In the following sections, the article looks at selected PTA provisions, particularly those involving "WTO-extra" issues, that we deem pertinent to shaping the regulatory environment while impacting human rights' protection through a detailed analysis of the most advanced electronic commerce chapters thus far — those of the CPTPP, the USMCA and the dedicated DEAs. We complement this analysis with an enquiry into the treaties of the European Union (EU), as the EU has been the leading regulator of data economy issues at home and the staunchest supporter of human rights protection. This should also provide a good understanding of how different stakeholders approach digital trade and its interfaces with human rights.

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

The CPTPP was agreed upon in 2017 between eleven countries in the Pacific Rim[17] and entered into force on December 30, 2018. The chapter on electronic commerce created at that point in time the most comprehensive template in the PTA landscape and was largely influenced by the U.S. during the Trans-Pacific Partnership Agreement negotiations,[18] from which the U.S. withdrew with the start of the first Trump administration.

In its first part and not unusually for US-led and other PTAs, the CPTPP electronic commerce chapter clarifies that it applies "to measures adopted or maintained by a Party that affect trade by electronic means"[19] 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.[20] The following provisions address, again as customarily, some of the

---

[17] Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore and Viet Nam.

[18] *See generally* Report on the Comprehensive and Progressive Agreement for Trans-Pacific Partnership, 72, Waitangi Tribunal of New Zealand (November 2021), https://forms.justice.govt.nz/search/Documents/WT/wt_DOC_104833137/Report%20on%20the%20Trans-Pacific%20Partnership%20Agreement%20W.pdf [hereinafter Waitangi Tribunal Report].

[19] Comprehensive and Progressive Agreement for Trans-Pacific Partnership, art. 14.2(2), Mar. 8, 2018, 3337 U.N.T.S. I-56101 [hereinafter CPTPP].

[20] *Id.* art. 14.2(3). For the lack of guidance and the potential contentions around the scope of this exception, see Waitangi Tribunal Report, *supra* note 18, at 81–83. For additional

leftovers of the 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 customs duties on electronic transmissions, including content transmitted electronically, and Article 14.4 endorses the non-discriminatory treatment of digital products,[21] which are defined broadly pursuant to Article 14.1.[22] 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 1996 or the UN Convention on the Use of Electronic Communications in International Contracts. The provisions on paperless trading and on electronic authentication and electronic signatures complement this by securing the equivalence of electronic and physical forms.[23]

The remainder of the provisions found in the CPTPP electronic commerce chapter belong to the category of rulemaking on data governance issues. Importantly, here the CPTPP explicitly seeks to curb data protectionism. First, it does so by including an explicit ban on the use of data localisation measures. Article 14.13(2) prohibits the parties from requiring a "covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory."[24] Second, the CPTPP includes a hard rule on free data flows in that: "[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."[25]

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."[26] These non-

---

exceptions, see *id.* arts. 14.2(4), (5) and (6).

[21] 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. *See* CPTPP, *supra* note 19, art. 14.2(3).

[22] CPTPP, *supra* note 19, art. 14.1. It defines a digital product as "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.

[23] CPTPP, *supra* note 19, arts. 14.9 and 14.6.

[24] *Id.* art. 14.13(2).

[25] *Id.* art. 14.11(2) (emphasis added).

[26] *Id.* art. 14.11(3). Further, it should be noted that the ban on localisation measures is

discriminatory conditions are similar to the general exceptions clauses under Article XIV of the GATS and Article XX of the General Agreement on Tariffs and Trade (GATT) 1994, which are intended to function as a balancing mechanism between trade and non-trade interests by "excusing" certain violations but involve a test that is also hard to pass, as the WTO jurisprudence has thus far revealed.[27] 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 speaks of a "legitimate public policy objective"[28] (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".[29]

The CPTPP addresses other novel issues as well — one of them is source code. Pursuant to Article 14.17, "[n]o Party shall 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."[30] The aim of this provision is to protect software companies and address their concerns, often linked with China, about forced technological transfer as a condition for market access.

The CPTPP chapter also has specific provisions with regard to the domestic regulatory frameworks. The provision on data protection is critical in this respect, as it 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."[31] Yet, there are no standards or benchmarks specified, except for a general requirement that CPTPP parties take into account principles or guidelines of relevant international bodies.[32] A footnote provides some clarification in saying that:

---

softened on financial services and institutions; government procurement is also excluded.

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

[28] CPTPP, *supra* note 19, art. 14.11(3).

[29] *See* General Agreement on Tariffs and Trade art. XX, April 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1A, 1867 U.N.T.S. 190 [hereinafter GATT]; General Agreement on Trade in Services, art. XIV, April 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183 [hereinafter GATS].

[30] *Id.* art. 14.17(2). On the possible interpretations of the provision and difference to including algorithms, see Waitangi Tribunal Report, *supra* note 18, at 104–112.

[31] CPTPP, *supra* note 19, art. 14.8(2).

[32] *Id.*

> . . . 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.[33]

Parties are also invited to promote compatibility between their data protection regimes by essentially treating lower standards as equivalent.[34] These provisions, while paying specific attention to privacy protection, can overall be interpreted as a prioritisation of trade over privacy rights. This was pushed by the U.S. during the TPP negotiations, as the U.S. subscribes to a relatively weak protection of privacy at home.[35]

Next to these important data protection provisions, the CPTPP also includes norms on consumer protection[36] and spam control,[37] as well as for net neutrality, which are, however, of a soft law nature.[38] Similarly, while cybersecurity is addressed, it only covers a limited scope of activities.[39]

The accession of the United Kingdom (U.K.) to the CPTPP in 2023 and the requests for accession by China, Taiwan, Costa Rica and others would potentially expand its commercial reach and geopolitical impact. Beyond this, it should be underscored that the CPTPP model has diffused to a substantial number of other agreements, such as the 2016 Chile-Uruguay Free Trade Agreement (FTA), the 2016 updated Singapore-Australia FTA, 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, 2019 Japan-U.S. DTA, and the 2020 Digital Economy Partnership Agreement (DEPA) between Chile, New Zealand, Singapore. The article discusses the post-CPTPP U.S. agreements, the DEAs, as well as the EU-led agreements to see how they measure against the CPTPP benchmark.

---

[33] *Id.* art. 19.8(2).
[34] *Id.* art. 14.8(5).
[35] *See*, *e.g.*, James Q. Whitman, *The Two Western Cultures of Privacy: Dignity versus Liberty*, 113 YALE L. J. 1151, 1151–1221 (2004); Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CAL. L.REV. 877–916 (2014); Mira Burri, *Interfacing Privacy and Trade*, 53 CASE W. REV. J. INT'L L. 35, 35–88 (2021) [hereinafter Burri III]; Anupam Chander & Paul M. Schwartz, *Privacy and/or Trade*, 90 U. CHI. L. REV. 49–135 (2023) [hereinafter Chander & Schwartz].
[36] CPTPP, *supra* note 19, art. 14.17.
[37] *Id.* art. 14.14.
[38] *Id.* art. 14.10.
[39] *Id.* art. 14.16.

C. The USMCA and the United States-Japan Digital Trade Agreement

After the withdrawal of the U.S. from the Trans-Pacific Partnership Agreement, there was some uncertainty as to the direction the U.S. would follow in its trade deals in general and on matters of digital trade in particular. The 2018 USMCA provided a useful confirmation of the U.S. approach. The USMCA comprehensive electronic commerce chapter, which was also properly titled "Digital Trade", followed all critical lines of the CPTPP[40] and created an even more ambitious template. Critically, for the article's discussion, the USMCA also ensures the free flow of data through a clear ban on data localisation[41] and a hard rule on free information flows.[42] 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.[43]

Beyond these similarities, the USMCA introduces some novelties. The first is that the USMCA departs from the standard U.S. approach and signals abiding to some data protection principles and guidelines of relevant international bodies. In the latter sense, parties are recommended to follow the Asia-Pacific Economic Cooperation (APEC) Privacy Framework and the Organisation for Economic Cooperation and Development (OECD) Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data.[44] In the former sense, the parties recognise key principles of data protection, which include: limitation on collection; choice; data quality; purpose specification; use limitation; security safeguards; transparency; individual participation; and accountability,[45] and aim to provide remedies for any violations.[46] This is interesting because it may go beyond what the

---

[40] With regard to replicating the CPTPP model, the USMCA follows the same broad scope of application, ban customs duties on electronic transmissions and binds the parties for non-discriminatory treatment of digital products. Furthermore, it provides for a domestic regulatory framework that facilitates online trade by enabling electronic contracts, electronic authentication and signatures, and paperless trading.

[41] Free Trade Agreement, U.S.-Mex.-Can., art. 19.12., Nov. 30, 2018, 134 Stat. 11 [hereinafter USMCA].

[42] *Id.* art. 19.11.

[43] *Id.* art. 19.11(2). There is a footnote attached, which clarifies that:

> 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.

[44] USMCA, *supra* note 41, art. 19.8(2).

[45] *Id.* art. 19.8(3).

[46] *Id.* arts. 19.8(4) and (5).

U.S. has in its national laws on data protection (at least so far[47]) 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.[48]

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"[49] and has become part of the ban on requirements for the transfer or access to source code in Article 19.16.[50] The second novum refers to the recognition of "interactive computer services" as particularly vital to the growth of digital trade. Parties pledge in this sense not to:

> adopt or maintain measures that treat a supplier or user of an interactive computer service as an information content provider in determining liability for harms related to information stored, processed, transmitted, distributed, or made available by the service, except to the extent the supplier or user has, in whole or in part, created, or developed the information.[51]

The third and rather liberal commitment of the USMCA parties is with regard to open government data. This is a forward-looking commitment of great relevance in the domain of domestic regimes for data governance, which recognises the importance of public access to and use of government information and seeks to enable it appropriately, including for businesses and for small and medium-sized enterprises specifically.[52]

The U.S. approach towards digital trade issues has also been confirmed by the 2019 U.S.-Japan DTA, signed alongside the U.S.-Japan Trade Agreement. The U.S.-Japan DTA can be said to replicate almost all provisions of the USMCA and the CPTPP,[53]

---

[47] Chander & Schwarz, *supra* note 35.
[48] Burri III, *supra* note 35.
[49] USMCA, *supra* note 41, art. 19.1.
[50] On the expansion of the scope of the source code provision, *see* Waitangi Tribunal Report, *supra* note 18, at 104–112.
[51] USMCA, *supra* note 41, art. 19.17(2). 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." *See also* Robert Wolfe, *Learning about Digital Trade: Privacy and E-Commerce in CETA and TPP*, 18 WORLD TRADE REV. 63–84 (2019) [hereinafter Wolfe].
[52] USMCA, *supra* note 41, art.19.8.
[53] *See generally* Digital Trade Agreement, U.S.-Jap., arts. 7, 8, 89, 10, 14, 11, 12, 16, 19, Oct. 7,

including the new USMCA rules on open government data,[54] source code,[55] and interactive computer services[56] but notably covering also financial and insurance services as part of the scope of the agreement. A new provision has been added regarding Information and Communications Technology (ICT) goods that use cryptography.[57] This additional ban on technological transfer is again a reaction to a practice by several countries, in particular China, which impose direct bans on encrypted products or set specific technical regulations that restrict the sale of encrypted products, and caters for the growing concerns of large companies, like IBM and Microsoft, which thrive on data flows with less governmental intervention.[58]

Other minor differences that can be noted when comparing with the USMCA are some things missing from the U.S.-Japan DTA, such as rules on paperless trading, net neutrality and the mention of data protection principles.[59] A final note deserves the exceptions attached to the U.S.-Japan DTA, which refer to the WTO general exception clauses of Article XIV of the GATS and Article XX of the GATT 1994, whereby the parties agree to their *mutatis mutandis* application[60] and do not follow the CPTPP or the USMCA template.

2019,
https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf [hereinafter U.S.-Japan DTA].

[54] *Id.* art. 20.

[55] *Id.* art. 17.

[56] *Id.* art. 18. A side letter recognises the differences between the U.S. 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.

[57] *Id.* art. 21. It specifies that for such goods designed for commercial applications, neither party shall require a manufacturer or supplier of the ICT good as a condition to entering the market to: (1) transfer or provide access to any proprietary information relating to cryptography; (2) partner or otherwise cooperate with a person in the territory of the Party in the development, manufacture, sale, distribution, import, or use of the ICT good; or (3) use or integrate a particular cryptographic algorithm or cipher.

[58] *See* Han-Wei Liu, *Inside the Black Box: Political Economy of the Trans-Pacific Partnership's Encryption Clause*, 51 J. WORLD TRADE 309–334 (2017).

[59] U.S.-Japan DTA, *supra* note 53, art. 15. This provision merely stipulates that parties shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade and publish information on the personal information protection, including how: (a) natural persons can pursue remedies; and (b) an enterprise can comply with any legal requirements.

[60] *Id.* art. 3. Further exceptions are listed with regard to security, prudential and monetary and exchange rate policy, and taxation which are to be linked to the expanded scope of agreement including financial and insurance services.

D. EU's Approach to Digital Trade

The EU has been a relatively late mover on digital trade issues and for a long time had not developed a distinct strategy, with earlier agreements largely concentrated on cooperation in the digital realm and some digital trade facilitation provisions,[61] while at the same time seeking commitments from its PTA partners to compatibility with the international standards of data protection.[62] Even in the 2016 EU agreement with Canada — the Comprehensive Economic and Trade Agreement (CETA) — while there were somewhat more commitments on digital trade,[63] there were not far-reaching and no discrete provisions addressed data.[64] This changed with the post-Brexit Trade and Cooperation Agreement (TCA) with the U.K.,[65] and the follow-up agreements with New Zealand and Chile, as well as the updated in 2023 EU-Japan FTA. These treaties include in their digital trade chapters norms on the free flow of data and data localisation bans. It is, however, the distinct approach of the EU to link these commitments with the high standards of personal data protection, as endorsed by its General Data Protection Regulation (GDPR)[66] and an understanding of privacy as a fundamental right, as embedded in EU's constitutional law.

So, while the EU and its partners seek to ban data localisation measures and subscribe to a free data flow (although not as fully as under the CPTPP/USMCA model[67]), 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."[68]

---

[61] *See generally* Free Trade Agreement, EC-Chile, Dec.18, 2002, O.J. (L 352); Free Trade Agreement, EU-South Korea, Oct.6, 2010, O.J. (L 127) 6–1343 [hereinafter EU-South Korea FTA].

[62] *See*, *e.g.*, EU-South Korea FTA, *supra* note 61, art. 7.48.

[63] *See*, *e.g.*, Comprehensive Economic and Trade Agreement, EU-Can., arts. 16:4 and 16:5, Oct. 30, 2016, O.J. (L. 11).

[64] *See*, *e.g.*, Wolfe, *supra* note 51.

[65] Trade and Cooperation Agreement, EU-UK, Jan. 30, 2020, O.J. (L. 149) 444/14 [hereinafter EU-UK TCA].

[66] Regulation 2016/679 of the European Parliament and of the Council of April 27, 2016, 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), O.J. (L 119) 1 [hereinafter GDPR].

[67] *See*, *e.g.*, Mira Burri & Kholofelo Kugler, *Regulatory Autonomy in Digital Trade Agreements*, 27 J. INT'L. ECON. L. 397, 397–423 (2024) [hereinafter Burri & Kluger].

[68] *See*, *e.g.*, Free Trade Agreement, EU-N.Z., art. 12.5(1), July 9, 2023, O.J. (L 886) [hereinafter EU-NZ FTA] (emphasis added). The EU-UK TCA has the specificity of no explicit mentioning of data protection as a fundamental right. This can, however, be presumed, since the UK incorporates the European Convention on Human Rights (ECHR) through the

Second, by a paragraph on data sovereignty that states "[e]ach 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."[69] The paragraph also makes clear that "[n]othing in this agreement shall affect the protection of personal data and privacy afforded by the Parties' respective safeguards."[70] 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.[71] In addition, there is a broad carve-out, in the sense that the following is provided:

> The Parties reaffirm each Party's right to regulate within their territories to achieve legitimate policy objectives, such as the protection of human, animal or plant life or health, social services, public education, safety, the environment, including climate change, public morals, social or consumer protection, animal welfare, privacy and data protection, the promotion and protection of cultural diversity, and, in the case of New Zealand, the promotion or protection of the rights, interests, duties and responsibilities of Māori.[72]

The EU thus reserves ample regulatory leeway for its current and future data protection measures.

In terms of the available exceptions, the EU also follows a distinct approach. To take the example of the latest EU treaty, the EU-Singapore Digital Trade Agreement (DTA), it incorporates the CPTPP-like legitimate public policy objectives (LPPO) exception but clarifies its scope through two footnotes. The first lists examples of legitimate public policy objectives that could justify exceptions that include:

> public security, public morals, or human, animal or plant life or health, (measures) to maintain public order, to protect other fundamental interests of society such as social cohesion, online safety, cybersecurity, safe and trustworthy artificial intelligence, or protecting against the

---

Human Rights Act of 1998 into its domestic law (although the UK may be shifting away from the Strasbourg model post-Brexit).

[69] *Id.* art. 12.5(2).

[70] *Id.*

[71] *Id.* art. 12.4(4).

[72] *Id.* art. 12.3. Specific for the EU-New Zealand FTA is the add-on "the promotion or protection of the rights, interests, duties and responsibilities of Māori." This addition is missing in the rest of the EU treaties.

> dissemination of disinformation, or other comparable objectives of public interest, taking into account the evolving nature of digital technologies and related challenges.[73]

This is the most detailed LPPO text thus far, even further-reaching than the fairly detailed updated EU-Japan FTA.[74] It certainly also goes beyond the closed list of policy objectives under the WTO general exceptions clauses and labels some concrete challenges of the digital era, as well as permits evolutionary interpretation.[75] The second clarification ensures that this provision does not influence the interpretation of other exceptions within the agreement.[76]

The rest of the EU digital trade template seems to include the issues covered by the CPTPP and the USMCA models, such as software source code,[77] facilitation of electronic commerce,[78] online consumer protection,[79] spam,[80] and open government data,[81] not including, however, a provision on non-discrimination of digital products, and excluding audio-visual services from the scope of the application of the digital trade chapter.[82]

E. The Digital Economy Agreements

Although, as earlier noted, PTAs have become more and more populated with dedicated digital trade provisions, they still are conventional trade agreements that cover a wide array of issues — including trade in goods, trade in services, IP

---

[73] Digital Trade Agreement, EU-Sing., art. 5(4), footnote 1, May 7, 2025 (provisional treaty version without prejudice) [hereinafter EU-Singapore DTA].

[74] Free Trade Agreement, EU-Japan, art. 8.81, Feb. 1, 2019, https://www.mofa.go.jp/ecm/ie/page4e_000875.html.

[75] Burri & Kluger, *supra* note 67.

[76] EU-Singapore DTA, *supra* note 73, art. 5(4) footnote 2.

[77] EU-UK TCA, *supra* note 65, art. 207. 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.

[78] *Id.* arts. 205, 206.

[79] *Id.* art. 208.

[80] *Id.* art. 209.

[81] *Id.* art. 210.

[82] *Id.* art. 197(2).

protection and sometimes, a variety of other issues, such as labour or environmental protection. There is, however, a new generation of treaties — the DEAs — that are monothematic and focus specifically on the regulation of digital trade and seek to provide a targeted regulatory framework. Since 2019, a total of six DEAs have been signed, and by September 2024, all these agreements entered into force. These encompass the 2019 US-Japan Digital Trade Agreement (DTA); DEPA, as the only plurilateral agreement, between Chile, New Zealand and Singapore and joined by South Korea in 2023; 2020 Australia-Singapore Digital Economy Agreement (ASDEA); 2022 UK-Singapore DEA; 2022 Korea-Singapore DEA and the 2023 UK-Ukraine DTA. The DEA landscape is now also joined by the EU with the 2025 EU-Singapore DTA and the 2025 EU-Korea DTA (both pending ratification and entry into force). This section takes the example of the DEPA[83] as one of the pioneering templates and the most comprehensive one so far to showcase the specificities of the DEA model.[84]

Importantly, and as already noted, DEAs are not conceptualised as a purely trade agreement but one that is meant to address the broader issues of the digital economy. Specifically, DEPA (but not the rest of the DEAs) is also not a closed deal but one that is open to other countries,[85] and meant to complement the WTO negotiations on electronic commerce and build upon the digital economy work underway within Asia-Pacific Economic Cooperation (APEC), the Organization for Economic Co-operation and Development (OECD), and other international forums. To enable flexibility and cover a wide range of issues, DEPA follows a modular approach that provides countries with more options to pick and choose and differs from the "all-or-nothing" approach of conventional trade treaties.[86]

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[87] (but not source code), and some of the US-Japan DTA

---

[83] For a comparison of the Digital Economy Partnership Agreement (DEPA) with existing PTAs, *see* Marta Soprana, *The Digital Economy Partnership Agreement (DEPA): Assessing the Significance of the New Trade Agreement on the Block*, 13 TRADE L. DEV. 143–169 (2021).

[84] For a fully-fledged analysis of all DEAs, *see* Mira Burri et al., *Understanding Digital Economy Agreements as a New Model of Trade Governance*, 52 LEGAL ISSUES ECON. INTEGRATION (forthcoming).

[85] Digital Economy Partnership Agreement, art. 16.2, June 12, 2020, https://www.mfat.govt.nz/assets/Trade-agreements/DEPA/Digital-Economy-Partnership-Agreement-DEPA-text.pdf [hereinafter DEPA].

[86] James Bacchus, *Special Report on the Digital Decide: How to Agree on WTO Rules for Digital Trade*, 8 CENTRE FOR INT'L GOVERNANCE INNOVATION (2021).

[87] DEPA, *supra* note 85, art. 9.4.

provisions, such as the one on ICT goods using cryptography,[88] 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,[89] 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.[90] 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 artificial intelligence (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-recognised principles or guidelines, including explainability, transparency, fairness, and human-centred values.[91] The DEPA parties also recognise the interfaces between the digital economy and government procurement and broader competition policy and agree to actively cooperate on these issues.[92] 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[93] 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.[94]

Overall, DEPA and the DEA model in general cover well the broad range of issues that the digital economy impinges upon and offers a good basis for interoperability of domestic frameworks and international cooperation that adequately considers the complex challenges of contemporary data governance that has essential trade but also non-trade elements. DEAs' appeal as a form of enhanced, but also flexible, cooperation has been confirmed by other agreements in the pipeline, such as

---

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

[89] *Id.* arts. 2.2 and 2.3. The provisions enumerate paperless trading and domestic electronic transactions framework respectively.

[90] *Id.* arts. 2.2, 2.5, 2.6, 2.4, and 2.7. These provisions demonstrate that 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).

[91] *Id.* art. 8.2(2) and (3).

[92] *Id.* arts. 8.3 and 8.4.

[93] *Id.* art. 9.2.

[94] *Id.* art. 11.2.

between Singapore and the European Free Trade Association (EFTA) members, as well as agreements that involve less developed countries, such as the Digital Economy Framework Agreement between the ASEAN members and the more advanced Digital Trade Protocol to the African Continental Free Trade Area (AfCFTA).[95]

Having in mind this sophisticated, albeit fragmented, framework for the regulation of digital trade issues, the following sections seek to unveil its human rights interfaces.

III. INTERFACES OF DIGITAL TRADE PROVISIONS AND HUMAN RIGHTS

A. Introduction

Trade and human rights have, in general, had a complex and contentious relationship.[96] While trade experts have maintained that human rights and trade law frameworks are mutually supportive,[97] human rights lawyers have rarely shared this opinion and felt that in different contexts, such as trade and climate change, trade and culture, trade and development, the hard rules of international trade law focus almost exclusively on economic values and do not sufficiently take into account the many interfaces or indeed right out ignore them.[98] The communication between the two camps has also not worked well so far,[99] and many issues of interfacing the two regimes remain unsettled.[100] Interesting in this debate and its evolution over time is the fact that the link between trade law and the first generation of human rights, like privacy or free speech, that this article discusses, has been seldomly touched upon.[101]

---

[95] On the AfCFTA Digital Trade Protocol, *See*, *e.g.*, Franziska Sucker, *Navigating Economic Inequalities Alongside African Digital Market Integration: The Role of the AfCFTA Competition Protocol*, 52 LEGAL ISSUES OF ECONOMIC INTEGRATION 5, 5–44 (2025).

[96] *See*, *e.g.*, Maya Hertig Randall, *Human Rights within a Multilateral Constitution: The Example of Freedom of Expression and the WTO*, 2012 MAX PLANCK Y.B. U.N. L., Vol. 16, at 186–187 [hereinafter Hertig Randall]. The work of Petersmann has particularly emphasised this positive dialogue. *See*, *e.g.*, Ernst-Ulrich Petersmann, *Human Rights, International Economic Law and Constitutional Justice*, 19 EUR. J. INT'L L. 769, 769–798 (2008).

[97] Hertig Randall, *supra* note 96 at 188.

[98] *Id.*

[99] Even going as far as saying that it has been "a dialogue of the deaf". *See* Hertig Randall, *supra* note 100 (citing *Linking Trade Regulation and Human Rights in International Law: An Overview*, *in* HUMAN RIGHTS AND INTERNATIONAL TRADE 7 (Thomas Cottier et al. eds., 2005).

[100] *See*, *e.g.*, Hertig Randall, *supra* note 96.

[101] As Hertig Randall points out, this may be because first generation rights, apart from the

It is not the article's objective to engage in a fully-fledged analysis of the interfaces between international trade and human rights regimes in general, but based on the above detailed enquiry into digital trade law provisions, to identify some more concrete implications of digital trade rules for the protection of fundamental rights. The following sections look first at the discussions around the privacy/data flows interface, which have also figured more prominently in the literature, and then sketch the less discussed implications for free speech and for development.

B. Digital Trade Law and Privacy Interfaces

Privacy and trade law have developed independently from each other, as their objectives and the tools of achieving them are profoundly different. Privacy protection can be framed as an individual right, while trade law has sought, reflecting the processes of economic globalisation, to enable the flow of goods, services, capital and less so people across borders. While both can be said to have their origins in the aftermath of the World War II – on the one hand, through providing for individual rights' protection against the state,[102] and through securing peace by regulating economic relations, on the other,[103] the rule-frameworks and the institutions created in the two domains are very different. The interfaces between privacy protection and trade law and the underlying tensions between sovereignty and international cooperation have not been common for a long time; neither have they been addressed in the legal frameworks.[104]

The interface between trade and privacy protection became relevant only with technological advances, which permitted the easy flow of information across borders and exposed the existing tensions.[105] During the late 1970s and the 1980s, as satellites, computers and software changed the dynamics of communications, the trade-offs between allowing data to flow freely and asserting national jurisdiction

---

right to property, were considered irrelevant for international trade. *See* Hertig Randall, *supra* note 96 at 189.

[102] *See*, *e.g.*, Thomas Cottier, *The Legitimacy The Law and Economics of Globalisation of WTO*, *in* THE LAW AND ECONOMICS OF GLOBALISATION 11–48 (Linda Yueh ed., 2009); PEACE AND PROSPERITY THROUGH WORLD TRADE: ACHIEVING THE 2019 VISION (Jean-Pierre Lehmann & Fabrice Lehmann eds., 2010).

[103] *See, e.g.,* PHILIP ALSTON & RYAN GOODMAN, INTERNATIONAL HUMAN RIGHTS (2012).

[104] GATT 1947 makes no reference to privacy and most of the free trade agreements up to very recently make no mention of it.

[105] *See, e.g.,* Christopher Kuner, *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future*, 187 OECD Digital Economy Paper (2011); Susan Aaronson, *Why Trade Agreements Are Not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights and National Security*, 14 WORLD TRADE REV. 672, 671–700, 680–685 (2015); Anupam Chander, *The Trade Origins of Privacy Law*, 99 IND. L. J. 649–674 (2024) [hereinafter Chander].

became readily apparent. Some states, echoing the concerns of large multinational companies, started to worry that barriers to information flows might seriously burden economic activities and looked for mechanisms that could prevent the erection of such barriers. It was clear that some sort of balancing mechanism was needed. Such a mechanism was found, in a soft legal form, in the principles elaborated under the auspices of the OECD.[106] The OECD framework, however, provides a bare minimum and readily permits diverging approaches to data protection, such as those of the EU and the US.[107] Moreover, as the OECD itself points out, while this privacy framework endured, the situation that we had in the 1970s and 1980s is profoundly different from the challenges in the realm of data governance we face today.[108] Pervasive digitisation and powerful hardware, coupled with the societal embeddedness of the Internet, have changed the volume, the intensity, and indeed, the nature of data flows.[109]

While the potential of data has been clearly acknowledged as a source of growth and innovation,[110] the increased dependence on data has brought about a new set of concerns. The impact of data collection and use upon privacy has been particularly widely acknowledged by scholars and policymakers alike, as well as felt by regular users of digital products and services.[111] These challenges have not been left unnoticed and have triggered the reform of data protection laws around the world, best exemplified by the EU GDPR and the diffusion of its model across

---

[106] OECD, *Guidelines for the Protection of Personal Information and Transborder Data Flows* (1980).
[107] *See, e.g.*, James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L. J. 1151; Paul M. Schwartz, *The EU-US Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966 (2013); Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CAL. L. REV. 877 (2014).
[108] OECD, *The OECD Privacy Framework: Supplementary Explanatory Memorandum to the Revised OECD Privacy Guidelines* (2013).
[109] *See* James Manyika et al., *Big Data: The Next Frontier for Innovation, Competition, and Productivity*, MCKINSEY GLOBAL INSTITUTE (June 2011) [hereinafter Manyika]; VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK (2013).
[110] *See, e.g.,* Manyika, *supra* note 109; Jacques Bughin et al., *Digital Europe: Pushing the Frontier, Capturing the Benefits*, (MCKINSEY GLOBAL INSTITUTE, June 2016).
[111] *See, e.g.,* The Obama White House, *Interim Report: Big Data: Seizing Opportunities, Preserving Values*, NATIONAL ARCHIVES (Feb. 13, 2015), https://obamawhitehouse.archives.gov/sites/default/files/docs/20150204_Big_Data_Seizing_Opportunities_Preserving_Values_Memo.pdf; Urs Gasser, *Recoding Privacy Law: Reflections on the Future Relationship Among Law, Technology, and Privacy*, 130 HARV. L. REV. 61–70 (2016); Directorate General of Human Rights and Rule of Law, *Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data*, COUNCIL OF EUROPE (2017), https://rm.coe.int/16806ebe7a.

jurisdictions.[112] The reform initiatives are, however, not coherent and are culturally and socially embedded, reflecting societies' deep understandings of constitutional values, relationships between citizens and the state, and the role of the market.

The tensions around data have also revived older questions about sovereignty and international cooperation in cyberspace.[113] Data's intangibility and pervasiveness pose particular difficulties for determining where data is located, as bits of data, even those associated with a single transaction or online activity, can be located anywhere.[114] With the increased value of data and the associated risks, and because of these contentious jurisdictional issues, governments have sought new ways to assert control over it — in particular by prescribing diverse measures that "localise" the data, its storage or suppliers, so as to keep it within the state's sovereign space.[115] This kind of erecting barriers to data flows impinges directly on trade and may endanger the realisation of an innovative data economy.[116] Data protectionism may also be associated with certain costs for the economy that endorses it.[117] Overall, with the amplified role of data in societies, the interfaces between trade and privacy

---

[112] *See, e.g.,* ANU BRADFORD, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD (2020); Chander, *supra* note 105; Graham Greenleaf, *The Brussels Effect* (Elgar Concise Encyclopedia of Privacy and Data Prot. L., 2025).

[113] For a great review of the theories on cyberspace regulation, their evolution over time and review of the literature, *see* Kristin E. Eichensehr, *The Cyber-Law of Nations*, 103 GEO. L. J. 317–380, 313–334 (2015). For a more recent analysis, *see* DATA SOVEREIGNTY: FROM THE DIGITAL SILK ROAD TO THE RETURN OF THE STATE (Anupam Chander & Haochen Sun eds., 2023) [hereinafter Chander & Sun].

[114] *See, e.g.,* Kristen E. Eichensehr, *Data Extraterritoriality*, 95 TEX. L. REV. 145, 145–160 (2017).

[115] *See, e.g.,* Anupam Chander, *National Data Governance in a Global Economy*, 495 UC DAVIS LEGAL STUDIES RESEARCH PAPER (2016), https://rb.gy/aos9be; Anupam Chander & Uyen P. Lê, *Data Nationalism*, 64 EMORY L. J. 677–739 (2015); Javier López González et al., *A Preliminary Mapping of Data Localisation Measures*, 262 OECD TRADE POLICY PAPERS (2022) https://www.oecd.org/en/publications/a-preliminary-mapping-of-data-localisation-measures_c5ca3fed-en.html; Graham Greenleaf, *Personal Data Localization and Sovereignty along Asia's New Silk Roads*, *in* DATA SOVEREIGNTY: FROM THE DIGITAL SILK ROAD TO THE RETURN OF THE STATE 295–331 (Anupam Chander & Haochen Sun eds., 2023) [hereinafter Greenleaf].

[116] Digital Trade in the U.S. and Global Economies, Inv. No. 332-531, USITC Pub. 4415 (July 2013) (Part 1); Digital Trade in the U.S. and Global Economies, Inv. No. 332-540, USITC Pub. 4485 (Aug. 2014) (Part 2); Greenleaf, *supra* note 115.

[117] *See, e.g.,* Richard D. Taylor, *"Data localization": The Internet in the Balance*, 44 TELECOMMUNICATIONS POLICY 102003 (2020); Martina F. Ferracane, *The Costs of Data Protectionism*, *in* BIG DATA AND GLOBAL TRADE LAW 63–82 (Mira Burri ed., 2021) [hereinafter Ferracane]. *But see* Svetlana Yakovleva & Kristina Irion, *Pitching Trade against Privacy: Reconciling EU Governance of Personal Data Flows with External Trade*, 10 INT'L DATA PRIVACY LAW 201, 201–221 (2020).

protection have become multiple and intensified, and this becomes clearly reflected in the new regime of digital trade that we mapped in the first part of the article. If one considers the rules on free data flows, including the ban on localisation measures, they do have a direct impact on the modalities of personal data protection as well as on the freedom of the sovereign state to maintain and adopt any measures to protect the privacy of its citizenry. As evident from the above PTA analyses, the approaches of states to handle these tensions vary significantly.

In particular, while we witness an increasing number of PTAs that prescribe the adoption of personal data protection frameworks and compliance with the existing international standards (which are mostly of a soft law nature)[118], the levels of commitment differ profoundly. This reflects the different domestic frameworks for privacy protection, which can be striking even between constitutional democracies such as the U.S. and the EU.[119] In the current landscape of digital trade law, it is only the EU that has, in accordance with its constitutional law, taken the necessary measures to ensure that the personal data protection of its citizens is also ensured in its external trade policy instruments. Not only does the EU include multiple safeguards in its PTAs, but it has also, as detailed above, calibrated the treaty exceptions in order to ensure that the digital trade commitments made, in particular with regard to cross-border data flows and data localisation requirements, would not stand in the way of existing and future data protection measures. Yet, the reference to privacy and personal data protection as a fundamental right has not become a staple in EU treaties, as initially foreseen in the Horizontal Provisions, agreed upon by EU stakeholders in 2018[120]. Only the EU-NZ FTA includes such explicit language in this regard — a divergence that has been criticised by European institutions, including the European Data Protection Supervisor.[121]

In addition, the EU ensures the protection of privacy outside of the trade regime through the adoption of unilateral adequacy decisions[122] that test the essential

---

[118] Out of the 465 PTAs in the TAPED dataset, 158 have provisions on data protection. Of them 59 are of hard and 99 of soft law nature.

[119] *See, e.g.,* Burri III, *supra* note 35; Chander & Schwartz, *supra* note 35.

[120] European Commission, *Horizontal Provisions for Cross-Border Data Flows and for Personal Data Protection (in EU Trade and Investment Agreements)*, EUROPEAN COMM. NEWSROOM (July 2018) https://ec.europa.eu/newsroom/just/items/627665/en.

[121] *Opinion 3/2024 on the Signing and Conclusion on Behalf of the European Union, of the Protocol Amending the Agreement between the European Union and Japan for an Economic Partnership Regarding Free Flow of Data*, EUROPEAN DATA PROTECTION SUPERVISOR, (Jan. 10, 2024), https://www.edps.europa.eu/data-protection/our-work/our-work-by-type/opinions_en.

[122] The European Commission has so far recognized Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom, the United States

equivalence of its partners' data protection regulation with the EU standards.[123] The squaring of these regimes is not always easy, as often EU trade partners are also parties to the CPTPP and DEAs that subscribe to different data governance norms. Japan, for instance, has an FTA as well as an adequacy decision with the EU, while at the same time being one of the main advocates for the APEC Cross-Border Privacy Rules System (CBPR), an initiative for cross-border data transfers spearheaded by the U.S. model of cross-border data transfer that has recently been transformed into the Global CBPR System, which is not restricted to APEC economies. Japan reconciles these apparent dual commitments through domestic legal mechanisms, and its data protection law contains a carve-out, by which EU citizens' data cannot be transferred to other APEC CBPR-participating economies using the APEC CBPR System (a practice known as "onward transfers").[124] Whether these adequacy decisions are sufficient to ensure truly adequate protection of EU citizens' data is however still an open question, as apart from the privacy frameworks with the US, none of the other adequacy schemes has been thus far challenged and tested in court. Yet, the experience gathered with the EU-U.S. Safe Harbour and its updates with the Privacy Shield and now the Transatlantic Data Privacy Framework may indeed point to insufficient safeguards and remedies. As it has been well-documented, both the Safe Harbour and the Privacy Shield, which functioned as self-certification schemes with certain monitoring and remedy mechanisms to ensure compliance with EU data protection, were found invalid, as they failed to provide sufficient protection for EU citizens' data and contrary to the EU Charter of Fundamental Rights.[125] The *Schrems* cases exemplify that, especially when there is

---

(commercial organisations participating in the EU–U.S. Data Privacy Framework) and Uruguay as providing adequate protection. *See generally* https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. There has been some interesting discussion as to whether the EU adequacy decisions are compatible with Article VII of the General Agreement on Trade in Services (GATS). *See* Maarja Saluste, *Cross-Border Data Adequacy Frameworks under GATS Article VII: Aligning WTO Members' Rights to Protect Personal Data with Their International Commitments,* 24 WORLD TRADE REV. 1, 1–27 (2025).

[123] GDPR, *supra* note 66, art. 45; *see also* Burri III, *supra* note 35; Chander & Schwartz, *supra* note 35. For a fully-fledged discussion, *see* SVETLANA YAKOVLEVA, GOVERNING CROSS-BORDER DATA FLOWS: RECONCILING EU DATA PROTECTION AND INTERNATIONAL TRADE LAW (2024).

[124] *See* Commission Implementing Decision (EU) 2019/419 of Jan. 23, 2019, Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Protection of Personal Data by Japan under the Act on the Protection of Personal Information, 2019 O.J. (L 76). *See also* Maria Vásquez Callo-Müller, *From APEC to Global: The Establishment of the Global CBPR Forum*, 20 GLOBAL TRADE & CUST. J. 130, 130–143 (2025).

[125] *See* Case C-362/14, Maximillian Schrems v. Data Prot. Comm'r (Schrems I), ECLI:EU:C:2015:650 (Oct. 6, 2015); Case C-311/18, Data Prot. Comm'r v. Facebook

legal activism that demands a closer scrutiny under EU constitutional law, the adequacy decisions may actually not survive the test. Anticipated developments in this context that can provide us with more insights will be a challenge of the Transatlantic Data Privacy Framework in a *Schrems III* case, especially now with the changed dynamics of the second Trump administration,[126] as well as the review of the UK's adequacy decision in 2026, specifically as the UK is now a CPTPP member and since the adoption of the EU-UK TCA has endorsed a liberal data governance stance in all its PTAs and DEAs.

Apart from the EU, when thinking about an adequate protection of privacy (and indeed other fundamental rights), two important points that deserve further discussion can be made. First, while data localisation has so far been framed as an obstruction to digital trade and data-driven growth and innovation,[127] there is an argument to be made that data localisation can in fact work both ways — as a limitation to liberties (functioning as enabler to censorship with both privacy and free speech implications, for instance) but also as a justified possibility for the state to protect the fundamental freedoms of its citizens (as in the EU example with personal data protection[128]). In this sense, as Chander and Sun point out, "[a]ssertions of digital sovereignty thus carry a double edge – as being useful both to protect citizens and to control them."[129]

Ireland Ltd. & Maximillian Schrems (Schrems II), ECLI:EU:C:2020:559 (July 16, 2020). The above cases rendered the agreements (Safe Harbor and Privacy Shield respectively) for data transfer between the U.S. and EU invalid on grounds that there were not enough safeguards and remedies in the U.S. for EU's citizens' data. *See also* Paul M. Schwartz, *The EU-US Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1966–2009 (2013); Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CAL. L. REV. 877, 877–916 (2014); Theodore Christakis, *European Digital Sovereignty, Data Protection, and the Push toward Data Localization*, *in* DATA SOVEREIGNTY: FROM THE DIGITAL SILK ROAD TO THE RETURN OF THE STATE 371–389 (Anupam Chander & Haochen Sun eds., 2023).

[126] The Data Privacy Framework did already "survive" its first review. *See Report from the Commission to the European Parliament and the Council on the First Periodic Review of the Functioning of the Adequacy Decision on the EU–US Data Privacy Framework*, COM(2024) 451 final (Oct. 9, 2024); *European Data Protection Board Report on the First Review of the European Commission Implementing Decision on the Adequate Protection of Personal Data under the EU–US Data Privacy Framework*, Version 1.1 (Nov. 4, 2024), https://www.edpb.europa.eu/our-work-tools/our-documents/other/edpb-report-first-review-european-commission-implementing_en.

[127] *See, e.g.,* Ferracane, *supra* note 117.

[128] *See, e.g.,* Anupam Chander, *Is Data Localization a Solution for Schrems II?,* 23 J. INT'L ECON. L. 771, 771–784 (2020); Elaine Fahey, *Does the EU's Digital Sovereignty Promote Localisation in Its Model Digital Trade Clauses?,* 8 EUROPEAN PAPERS 503, 503–511 (2023).

[129] Chander & Sun, *supra* note 113, 72–88; Henry Gao, *Data Sovereignty and Trade Agreements: Three Digital Kingdoms*, *in* Chander & Sun, *supra* note 113.

Second, the existing reconciliation models that we have thus far in the form of general exception clauses under WTO law[130] and in modified versions under PTAs[131] are of still uncertain value. Despite the fact that, especially in the post-CPTPP landscape, we have seen a clear rise in coupling digital trade commitments with exceptions and other flexibilities,[132] there is still no relevant jurisprudence so far, under the WTO or elsewhere. Furthermore, despite increased scholarly and policy attention paid, the scope of the exceptions in PTAs remains unclear – for instance and as discussed earlier, the CPTPP and the USMCA refer to "a legitimate public policy objective" without any enumeration of such objectives, which can be linked to legal uncertainty but also to insufficient safeguards for domestic constituencies. This was clearly acknowledged by the Waitangi Tribunal in New Zealand with regard to the protection of the data governance of the Māori people,[133] as the CPTPP could restrict the adoption of Tiriti-based governance and protections in the future and prejudice Māori Tiriti rights, interests and responsibilities in relation to Māori knowledge, authority and power and the exercise of Māori law.[134] For this reason, in later agreements of New Zealand, there is a specific exception framed for indigenous people.[135]

To sum up with regard to the privacy/digital trade law interface, while it can be welcomed that the implications of digital trade with underlying cross-border data flows and the protection of personal data have become duly acknowledged, the regulatory framework that has emerged is still lacking. In this context, it has been discussed whether there is a distinct need to provide for minimum standards of privacy protection at the international level, either through a substantive treaty or through a procedural one that can be linked to the WTO dispute settlement.[136] Others have argued in contrast, that data privacy should not be put in trade law at all.[137] As under the current geopolitics, both scenarios appear unlikely, we remain faced with a picture of profound fragmentation, with the data protection and digital trade law frameworks developing at different speeds and with the EU as the only

---

[130] GATT, art. XX, *supra* note 29; GATS, art. XIV, *supra* note 29.
[131] *See* Burri III, *supra* note 35.
[132] For a fully-fledged analysis, see Burri & Kluger, *supra* note 67.
[133] Waitangi Tribunal Report, *supra* note 18, at 132–142.
[134] *Id.*
[135] EU-NZ FTA, *supra* note 68, art. 12.3. *See also* Mira Burri et al., *Digital Trade in the EU–New Zealand FTA: An Appraisal,* 51 LEGAL ISSUES OF ECON. INTEGRATION 11, 11–46 (2024).
[136] Chander & Schwartz, *supra* note 35.
[137] *See, e.g.,* Kristina Irion et al., *Privacy Peg, Trade Hole: Why We (Still) Shouldn't Put Data Privacy in Trade Law*, UNI. OF CHI. REV. ONLINE (Mar. 27, 2023), https://lawreviewblog.uchicago.edu/2023/03/27/irion-kaminski-yakovleva/.

party making sure that proper interfaces are made and safeguards provided.

C. Digital Trade Law and Free Speech Interfaces

As a starting point in this context, one can criticise the sole focus on privacy under digital trade law, while downplaying other fundamental rights and freedoms, such as freedom from discrimination, equality, minority rights and free speech. In the discrete context of the latter, in somewhat older debates trade law scholars have explored the utility of trade rules to address situations of censorship, as these may qualify as violations of WTO rules and commitments and as the trade law framework provides stronger enforcement mechanisms than those available under international human rights law.[138] This idea of "[i]f prying open markets is a way to pry open minds, WTO trade obligations can be used to limit censorship",[139] was however later on undone in the *China — Audiovisual Products* case.[140] There, China was ultimately allowed to pursue its censorship regime under the GATT Article XX "public morals" exception, albeit through a less trade-restrictive manner — oddly enough, by "nationalising" the censorship — which is certainly not the outcome free speech advocates were hoping for.[141] Beyond this dispute, it has been argued there is "only partial and weak support for a conceptual confluence between liberal trade and the human right of free speech"[142]. Moreover, as Broude and Hestermeyer state:

> [f]or the WTO, and indeed for other trade agreements, taking up the cause of the freedom of speech would be too heavy a burden, and one that would merely be harmful to its overarching legitimacy. No less importantly, for human rights, and especially for rights advocates, it is clearly dangerous to make instrumental

---

[138] *See, e.g.,* Tim Wu, *The World Trade Law of Censorship and Internet Filtering,* 7 CHI. J. INT'L L. 263–287 (2006); Anupam Chander, *International Trade and Internet Freedom*, 102 AMERICAN SOCIETY OF INT'L L. 37, 37–49 (2008); Brian Hindley & Hosuk Lee-Makiyama, *Protectionism Online: Internet Censorship and International Trade Law*, (European Ctr. For Int'l Political Economy, Working Paper No. 12, 2009); Henry Gao, *Googling for the Trade–Human Rights Nexus in China: Can the WTO Help?, in* TRADE GOVERNANCE IN THE DIGITAL AGE 247–275 (Mira Burri & Thomas Cottier eds., 2012).

[139] Joost Pauwelyn, *Squaring Free Trade in Culture with Chinese Censorship: The WTO Appellate Body Report on China — Audiovisuals*, 11 MELB. J. INT'L L. 123, 119–140 (2010) [hereinafter Pauwelyn].

[140] 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 19 January 2010).

[141] *See* Pauwelyn, *supra* note 139; Paola Conconia & Joost Pauwelyn, *Trading Cultures: Appellate Body Report on China — Audiovisuals*, 10 WORLD TRADE REV. 95, 95–118 (2011).

[142] Tomer Broude & Holger P. Hestermeyer, *The First Condition of Progress — Freedom of Speech and the Limits of International Trade Law*, 54 VA. J. INT'L L. 304, 295–321 (2014).

use of trade law for the promotion of the freedom of expression.[143]

These discussions are certainly valuable. Yet, they have not been updated to take into account the profound changes in either the digital media space or in digital trade law, as transformed in recent years. In the former context, a phenomenon that has captured the attention of both scholars and policymakers is the critical role played by platforms.[144] Platforms like social networking sites, search engines and other types of aggregators, often driven by algorithms, have turned into gatekeepers in contemporary media environments. In such a configuration, nation states tend to create different liability regimes for digital companies that may trigger collateral censorship and prior restraint. Social media companies in their own right create sophisticated systems of private governance that regulate users arbitrarily and without due process and transparency. At the same time, users are highly vulnerable to digital surveillance and manipulation, and the intensified datafication of the digital economy only exacerbates this vulnerability.[145] Another element that complicates the conditions of free speech in the era of platforms is their staggering power, vis-à-vis the states (both domestic and foreign regulators), vis-à-vis other companies on the same or adjacent markets, and ultimately vis-à-vis users. Indeed, it has been argued that platforms have become the "new governors"[146] or the "emergent transnational sovereigns" of the digital space.[147] This power is often unchecked and platforms moderate speech practice and cultural communication and engagement with accountability neither to their users nor to state agencies.[148] The power of platforms and their deep impact on communicative processes within a society have become problematic and particularly palpable with the proliferation of fake news and the formation of the so-called "echo chambers", which destroy the very virtues of a digitally enabled global sphere and lead to a fragmentation of the public

---

[143] *Id.*

[144] *See, e.g., Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions online platforms and the digital single market opportunities and challenges for Europe*, COM(2016) 288 final (May 5, 2016); Orly Lobel, *The Law of the Platform*, 101 MINN. L. REV. 87, 87–166 (2016); Julie E. Cohen, *Law for the Platform Economy*, 51 U.C. DAVIS L. REV. 133, 133–204, (2018) [hereinafter Cohen]; Jack M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. DAVIS L. REV. 1149, 1149–1210 (2018) [hereinafter Balkin I]; Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598, 1598–1670 (2018) [hereinafter Klonick]; RASMUS KLEIS NIELSEN & SARAH A. GANTER , THE POWER OF PLATFORMS SHAPING MEDIA AND SOCIETY (2022).

[145] *See, e.g.,* Balkin I, *supra* note 144; Klonick, *supra* note 144; Jack M. Balkin, *Free Speech Is a Triangle*, 118 COLUM. L. REV. 2011, 2011–2055 (2018) [hereinafter Balkin II].

[146] Balkin II, *supra* note 145; Klonick, *supra* note 144.

[147] Cohen, *supra* note 144.

[148] *See, e.g.,* Balkin I, *supra* note 144; SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019).

discourse and possible polarization of views.[149] Regulators around the world have realised these grave implications, and at least in some jurisdictions (notably the EU), there are discrete and far-reaching regulatory responses,[150] while the challenge of AI speech still remains to be (partially or fully) addressed.[151]

In the trade law context, scattered provisions in the newer generation of PTAs and DEAs can be deemed relevant against this backdrop. On the one hand, a number of treaties have included provisions on open government data and on internet access[152] that can be deemed as supportive of the conditions of free speech practice. Further in this positive context, we have provisions, although only of soft legal nature, on digital inclusion with a goal to enable participation and improve access for women, rural populations and low socio-economic groups,[153] as well as provisions that recognise the importance of a rich and accessible public domain.[154] On the other hand, one can also observe a sizeable reduction of policy space through digital trade commitments, which may be driven by the very interests of the powerful

---

[149] *See, e.g.,* CASS R. SUNSTEIN, GOING TO EXTREMES: HOW LIKE MINDS UNITE AND DIVIDE (2009); *Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Action Plan Against Disinformation*, JOIN (2018) 36 final (Dec. 5, 2018); House of Commons: Digital, Culture, Media and Sport Committee, *Disinformation and "Fake News": Final Report*, U.K. PARL. (Feb. 18, 2019), https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf; Joshua A. Tucker et al., *Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature*, HEWLETT FOUNDATION (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3144139; Lance W. Bennett & Steve Livingston, *The Disinformation Order: Disruptive Communication and the Decline of Democratic Institutions*, 33 EUR. J. COMM. 122, 122–139 (2018); Viorela Dan et al., *Visual Mis- and Disinformation*, 98 JOURNALISM AND MASS COMM. Q. 641, 641–664 (2021).

[150] *See, e.g.,* Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), 2022 O.J. (L 277) 2022) [hereinafter DSA]. *See also* Mira Burri, *Fake News in Times of Pandemic and Beyond: Exploring of the Rationales for Regulating Information Platforms*, *in* LAW AND ECONOMICS OF THE CORONAVIRUS CRISIS 31–58 (Klaus Mathis & Avishalom Tor eds., 2022) [hereinafter Burri IV].

[151] *See, e.g.,* Margot E. Kaminski & Meg Leta Jones, *Constructing AI Speech*, 133 YALE L. J. F. 1212, 1212–1266 (2024); Tomas Dodds et al., *Popularity-Driven Metrics: Audience Analytics and Shifting Opinion Power to Digital Platforms*, 23 JOURNALISM STUD. 403, 403–421 (2023). *See also* Natali Helberger*, FutureNewsCorp, or How the AI Act Changed the Future of News*, 52 COMP. L. & SEC. REV. 105915 (2024); Natali Helberger & Nicholas Diakopoulos, *The European AI Act and How It Matters for Research into AI in Media and Journalism*, 11 DIGITAL JOURNALISM 1751, 1751–1760 (2022).

[152] *See, e.g.,* USMCA *supra* note 41, DEPA *supra* note 85; EU-UK TCA, *supra* note 65.

[153] *See, e.g.,* DEPA, *supra* note 85, art. 11.1. *See* discussion infra part III.D.

[154] *See, e.g.,* DEPA, *supra* note 85, art. 9.3.

players and may constrain public interest-oriented regulatory action going forward.[155] Two distinct types of rules can be highlighted in this context. The first category covers the now increasingly common provisions on source code,[156] which seek in essence to ban forced technological transfer and thus provide for business trust. These norms tend to be broadly defined, and in some agreements, now also include algorithms.[157] Simultaneously, the exceptions to the prohibition on requiring access to source code are comparatively narrow and do not cover the multitude of reasons why public authorities might legitimately want access to source code — to ensure equality, privacy and consumer protection or any other type of action in the public interest.[158] The second type of rules on "interactive computer services" are more specific to freedom of expression and can only be found so far exclusively in U.S. trade deals.[159] This provision is important, as it limits the liability of intermediaries for third-party content and, in essence, secures the application of Section 230 of the U.S. Communications Decency Act[160] that creates an almost perfect safe harbour for platforms, while also permitting content moderation practices. Both the act of imposing the U.S. domestic standards of free speech on other countries,[161] which may share different from the First Amendment

---

155 For an especially outspoken view, *see* Deborah James, *Global Trade Rules: A Disastrous New Constitution for the Global Economy*, CTR. FOR ECON. & POL. RESEARCH (2020), https://cepr.net/wp-content/uploads/2020/07/digital-trade-2020-07.pdf [hereinafter James].

156 *See, e.g.,* CPTPP, *supra* note 19; USMCA, *supra* note 41; US-Japan DTA, *supra* note 53; DEPA, *supra* note 85; EU-UK TCA, *supra* note 65.

157 *See, e.g.*, USMCA, *supra* note 41, art. 19.16; US-Japan DTA, *supra* note 53, art. 17. On the expansion of the scope of the source code provision, see Waitangi Tribunal Report, *supra* note 18, at 104–112.

158 James, *supra* note 155; Cosimina Dorobantu et al., *Source Code Disclosure: A Primer for Trade Negotiators*, *in* ADDRESSING IMPEDIMENTS TO DIGITAL TRADE 105–140 (Ingo Borchert et al. eds., 2021).

159 USMCA, *supra* note 41, art. 19.17(2); US-Japan DTA, *supra* note 53, art. 18.

160 Communications Decency Act § 230, Pub. L. No. 104–104 (Tit. V), 110 Stat. 133 (1996). 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." *See, e.g.,* Eric Goldman, *Why Section 230 Is Better Than the First Amendment*, 95 NOTRE DAME L. REV. REFLECTION 33, 33–46 (2019); Eric Goldman, *An Overview of the United States' Section 230 Internet Immunity*, *in* THE OXFORD HANDBOOK OF ONLINE INTERMEDIARY LIABILITY 155–171 (Giancarlo Frosio ed., 2020); Tanner Bone, *How Content Moderation May Expose Social Media Companies to Greater Defamation Liability*, 98 WASH. U. L. REV. 937, 937–963 (2021).

161 Such a practice has been particularly common in the area of IP protection. *See, e.g.,* SUSAN K. SELL, PRIVATE POWER, PUBLIC LAW: THE GLOBALIZATION OF INTELLECTUAL PROPERTY RIGHTS (2009); Margot E. Kaminski, *The Capture of International Intellectual Property Law Through the U.S. Trade Regime*, 33 S. CAL. L. REV. 977, 977–1052 (2014).

traditions,[162] as well as the platforms' safe harbour in itself, can be viewed as problematic. The liability safe harbour that has been recently under attack (even in the U.S.)[163] and has become constrained through regulatory action in many jurisdictions in the face of fake news and other negative developments related to platforms' power.[164] The EU has again been in this context the leading regulatory entrepreneur at home with a number of far-reaching legislative actions of both soft and hard legal nature, such as the Digital Services Act (DSA)[165] or the Digital Markets Act (DMA),[166] amongst others. In contrast to efforts in the area of personal data protection, these have not been reflected in the new generation of EU digital trade treaties, except for a new mention of "dissemination of disinformation" in the exemplary list of legitimate public policy objectives.[167] And perhaps there are good

---

[162] *See, e.g.,* Claudia E. Haupt, *Regulating Hate Speech: Damned If You Do and Damned If You Don't – Lessons Learned from Comparing the German and U.S. Approaches*, 23 BOSTON UNIV. INT'L L. J. 300, 300–335 (2005) (also providing an overview of the comparative literature); Ionna Tourkochoriti, *Speech, Privacy and Dignity in France and in the U.S.A.: A Comparative analysis*, 38 LOY. L.A. INT'L & COMP. L.REV. 101, 101–182 (2016).

[163] In 2023, two U.S. Supreme Court decisions dealt with Section 230 of the Communications Decency Act, 1996. *Gonzalez v. Google LLC*, 598 U.S. 617 (2023) [hereinafter Gonzalez] dealt with the question of whether or not recommender systems are covered by liability exemptions under Section 230 in dealing with terrorism-related content posted by users and hosted on their servers. The case was granted certiorari alongside another terrorism-related case, *Twitter, Inc. v. Taamneh,* 598 U. S. 471 (2023) [hereinafter Twitter]. In May 2023, the court ruled unanimously in *Twitter* that the charges against the social media companies were not permissible under antiterrorism law; *Gonzalez* was sent back to lower courts on a *per curiam* decision with instructions to consider the Court's decision in *Twitter*. Section 230 remained ultimately unaffected. More recently, with regard to the application of the First Amendment to platforms, the U.S. Supreme Court upheld the Protecting Americans from Foreign Adversary Controlled Applications Act (PAFACA) that could effectively ban TikTok in the US, unless its Chinese parent company, ByteDance, sells (80%) to a US-based entity and rejected TikTok's First Amendment challenge of the law. *See TikTok, Inc. v. Garland*, 604 U.S. ___ (2025).

[164] *See, e.g.,* Burri IV, *supra* note 150.

[165] DSA, *supra* note 154.

[166] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), 2022 O.J. (L 265) [hereinafter DMA].

[167] *See* EU-Singapore DTA, *supra* note 73, art. 25, at footnote 1. It provides that:

> For the purpose of this Article, legitimate public policy objective shall be interpreted in an objective manner and shall enable the pursuit of objectives such as to protect public security, public morals, or human, animal or plant life or health, to maintain public order, to protect other fundamental interests of society such as social cohesion, online safety, cybersecurity, safe and trustworthy artificial intelligence, or protecting against the dissemination of disinformation, or other

reasons for this.[168] Still, at this point in time, critical developments with human rights implications, such as data-sharing, algorithmic decision-making, censorship and internet shutdowns, limiting disinformation and private power remain currently unaddressed in data governance rules as designed in trade forums.[169]

D. Digital Trade Law and Development Interfaces

So far, PTAs' digital trade chapters have not sought to make a direct link to development, at least not in the way provided for in the environment, labour or gender chapters of some treaties. While one can subsume the commitments on consumer protection, business trust and especially digital trade facilitation under the category of beneficially contributing, there is no clear treaty language to this effect. Yet, this somewhat grim picture may be changing, as a number of newer agreements place specific emphasis on development. This is particularly evident in a select few PTAs and especially in the DEAs, and this article showcases this new development by focusing on the provisions on digital inclusion.

Currently, twelve treaties include provisions on digital inclusion.[170] While this

---

comparable objectives of public interest, taking into account the evolving nature of digital technologies and related challenges.

[168] *See, e.g.,* Anupam Chander, *When the Digital Services Act Goes Global*, 38 BERKELEY TECH. L. J. 1067, 1067–1088 (2025).

[169] *See, e.g.,* Susan Aaronson, *The Difficult Past and Troubled Future of Digital Protectionism*, *in* ADDRESSING IMPEDIMENTS TO DIGITAL TRADE 141–168 (Ingo Borchert et al. eds., 2021); Svetlana Yakovleva & Joris van Hoboken, *The Algorithmic Learning Deficit: Artificial Intelligence, Data Protection and Trade*, *in* BIG DATA AND GLOBAL TRADE LAW 212–230 (Mira Burri ed., 2021).

[170] DEPA, *supra* note 85, art. 11.1; Free Trade Agreement, Chile-Paraguay, art. 7.22, Dec. 1, 2021, https://edit.wti.org/document/show/6c1d59c5-a57f-42b6-baec-4ffea1a7c7d6; Comprehensive Economic Partnership Agreement, India-U.A.E., art. 9.13(2)(a), Feb. 18, 2022, https://www.moec.gov.ae/documents/20121/1347101/Final+Agreement_UAE+India+CEPA.pdf [hereinafter India-UAE CEPA]; Digital Economy Agreement, Sing.-U.K., art. 8.61-P, June. 14, 2022, CS Singapore No.1/2022 [hereinafter UK-Singapore DEA]; Free Trade Agreement, U.K.-N.Z., art. 15.20, Feb. 28, 2022, https://www.mfat.govt.nz/assets/Trade-agreements/UK-NZ-FTA/NZ-UK-Free-Trade-Agreement.pdf [hereinafter UK-NZ FTA]; Digital Trade Agreement, U.K.-Ukraine, art. 132-T, Feb. 20, 2023, https://www.gov.uk/government/publications/ukukraine-digital-trade-agreement-cs-ukraine-no22023; Second Protocol to Amend the Agreement Establishing the ASEAN-Australia-New Zealand Free Trade Area, Aug. 21, 2023, art. 10.19, https://www.dfat.gov.au/sites/default/files/second-protocol-to-amend-the-agreement-establishing-the-asean-australia-new-zealand.pdf; Free Trade Agreement, China-Nicar., art. 12.8(3)(d), Aug. 31, 2023, https://fta.mofcom.gov.cn/topic/ennicaragua.shtml; Free Trade Agreement, Can.-Ukr., art. 23.4(5)(d), Sept. 22, 2023, https://www.international.gc.ca/trade-

number still appears relatively small, it should be noted that in 2022, only five of the then 379 surveyed PTAs included such a provision. The provisions in all treaties are largely formulated as cooperation/promotion of digital inclusion, so they are of a soft legal nature. The 2022 UK-New Zealand FTA, which specifically addresses the digital divide and inclusion, is notable for its somewhat "harder" language. It says that the parties *shall* cooperate on matters relating to digital inclusion, including participation of Māori, women, persons with disabilities, rural populations, and low socio-economic groups as well as other individuals and groups that disproportionately face barriers to digital trade.[171] Such a cooperation may include: (a) enhancing cultural and people-to-people links, including for Māori, through promoting business development services; (b) identifying and addressing barriers to accessing digital trade opportunities; (c) improving digital skills and access to online business tools; and (d) sharing methods and procedures for developing datasets and conducting analysis to identify barriers and trends over time in relation to Māori, women, and other groups which face barriers to digital trade to inform the development of digital trade policies, including developing methods for monitoring their participation in digital trade.

In the follow-up section, there is also particular attention paid to the role played by micro-, small and medium-sized enterprises (MSMEs), including Māori-led and women-led enterprises, in economic growth and job creation, and the need to address the barriers to participation in digital trade for those entities.[172] Notably, there is also the commitment of the parties to bridging the digital divide in developing countries (that is, countries other than the treaty parties) — not only to enable their participation in digital trade but also in digital trade rulemaking. In this sense, the parties commit, although in a soft law manner, to undertake and strengthen cooperation, including through existing mechanisms, to promote the participation of developing countries in digital trade. This may include sharing best practices, active engagement in international fora, and promoting developing countries' participation in, and contribution to, the global development of rules on digital trade, which may include other WTO members as appropriate.[173] Almost

---

commerce/trade-agreements-accords-commerciaux/agr-acc/ukraine/text-texte/2023/toc-tdm.aspx?lang=eng [hereinafter Canada-Ukraine FTA]; AfCFTA Digital Trade Protocol, art. 30, Feb. 18, 2024, https://www.bilaterals.org/IMG/pdf/afcfta_digital_trade_protocol_-_9_february_2024_draft.pdf [hereinafter AfCFTA Digital Protocol]; Comprehensive Economic Partnership Agreement, Austl.-U.A.E., art. 12.25, Nov. 6, 2024, https://www.dfat.gov.au/trade/agreements/not-yet-in-force/australia-uae-comprehensive-economic-partnership-agreement-cepa/australia-uae-cepa-official-text [hereinafter Australia-UAE CEPA]; EU-Singapore DTA, *supra* note 73, art. 25.

[171] UK-NZ FTA, *supra* note 170, art. 15.20(2) (emphasis added).

[172] *Id.* art. 15.20(3).

[173] *Id* art. 15.20(4). *See* also Department for International Trade and Department for Business

identical provisions are to be found in the UK–Singapore DEA,[174] with one interesting add-on regarding the promotion of "labour protection for workers who are engaged in or support digital trade."[175]

The language of the DEPA is also similar, but does not include this last commitment.[176] One thing that stands out in the DEPA, however, is the link to multi-stakeholder participation, as the DEPA clarifies that digital inclusion cooperation activities "may be carried out through the coordination, as appropriate, of the Parties' respective agencies, companies, labour unions, civil society, academic institutions, and non-governmental organisations, among others."[177] While the trend of more detailed digital inclusion provisions is evident in DEAs as a new particular type of treaties, it is not a standard feature of all DEAs — the US-Japan DTA, Singapore-Australia and Korea-Singapore DEAs do not contain such a provision. At the same time, less visible agreements, involving developing countries, have started to address digital inclusion. For instance, the United Arab Emirates (UAE) has two PTAs with India[178] and Australia,[179] respectively. One also needs to mention in this context the AfCFTA Digital Trade Protocol, which contains a dedicated part focused on digital trade inclusion with four articles addressing digital inclusion; MSMEs, digital innovation and entrepreneurship, and digital skills development.[180] While there are some overlaps with other treaty language on digital inclusion, it is noteworthy that the provisions on MSMEs and digital innovation specifically mention access to finance as well as underscore the need for adequate policy, legal and institutional frameworks. The AfCFTA Digital Trade Protocol is also the only treaty thus far with a dedicated article on digital skills development,[181] as well as the only one with a provision on digital infrastructure.[182]

Overall, one can undoubtedly welcome these new developments and the increased

---

and Trade, *Inclusive Trade in the UK-New Zealand Free Trade Agreement*, GOVT. U.K. (Feb. 28, 2022), https://www.gov.uk/government/publications/uk-new-zealand-fta-inclusive-trade-explainer.

[174] UK-Singapore DEA, *supra* note 170, art. 8.61-P.

[175] *Id* art. 8.61-P(2)(e).

[176] DEPA, *supra* note 85, Module 11.

[177] *Id.* module 11(4). A more generic formulation with similar meaning can be found in the UK–Singapore DEA, *supra* note 170.

[178] *See* India-UAE CEPA, *supra* note 170, art. 9.13.

[179] *See* Australia-UAE CEPA, *supra* note 170, art. 12.25.

[180] AfCFTA Digital Protocol, *supra* note 170, arts. 30, 31, 32 and 33.

[181] *Id.* art. 33. Digital skills in other agreements are often part of the digital inclusion provisions. They can sometimes be found in other parts of the treaty. *See, e.g.,* Canada-Ukraine FTA, *supra* note 170, art. 24.4. It specifically mentions cooperation on fostering women's digital skills and access to online business tools in the chapter on trade and gender.

[182] AfCFTA Digital Protocol, *supra* note 172, art. 18.

engagement with digital inclusion. Yet, there is the lingering question of whether this is sufficient. The answer is a clear 'no', for a number of reasons. First, as already noted, the majority of the provisions that we have are of a soft law nature — even the "shall cooperate" language does not create a real obligation for the parties. Nor are there any monitoring or other measures in case of non-compliance. Another concern, which has been highlighted by other scholars too,[183] is the lack of meaningful commitments on capacity building of either regulatory or technical nature. While it is expected that developing countries participate in digital trade rulemaking and enter into far-reaching commitments in the domain of data governance, there is, in return, no regulatory assistance or technical support. Agarwal and Mishra argue that "[n]o trade agreement, involving two or more countries placed at different stages of the developmental ladder, can be practical in the absence of meaningful provisions on [special and differential treatment] SDT."[184] It is also important that this type of SDT must go beyond the postponement of the implementation of specific provisions by developing countries and LDCs, as increasingly included in treaties, as well as have a more binding legal nature.[185] In the latter sense, in the context of the WTO eJSI negotiations, there is a meaningful proposal on SDTs formulated by Côte d'Ivoire (with additions from Indonesia and China)[186] suggesting the introduction of enforceable provisions on capacity building and technical assistance for developing countries and LDCs, along the lines of the WTO Trade Facilitation Agreement, which provides for enforceable capacity-building and technical assistance and self-designated transitional implementation periods, as well as linking the implementation of some commitments to the provision of technical and capacity-building assistance.

The 2025 Agreement on Electronic Commerce, adopted under the eJSI framework, although a remarkable advancement in linking digital trade regulation and development, does not go that far.[187] Article 20 herein is important, as it clearly acknowledges the need for technical assistance and capacity building in order to enable an inclusive digital economy. Yet, most of the provisions in this context are

---

[183] *See, e.g.,* NEHA MISHRA, INTERNATIONAL TRADE LAW AND GLOBAL DATA GOVERNANCE: ALIGNING PERSPECTIVES AND PRACTICES (2024); Agarwal & Mishra, *supra* note 9; Fabio Morosini et al., *Navigating the Digital Divide: Challenges and Strategies for Latin American Countries in E-Commerce and Data Governance Regulation*, GEORGETOWN L. (2024), https://www.law.georgetown.edu/carola/wp-content/uploads/sites/29/2024/11/2024-LAPEG_1_Policy-Brief-Digital-Trade.pdf [hereinafter Morosini].

[184] Agarwal & Mishra, *supra* note 9.

[185] Morosini, *supra* note 183.

[186] World Trade Organization, Joint Statement on Electronic Commerce: Communication from Côte d'Ivoire, WTO Doc. INF/ECOM/49 (Dec. 16, 2019).

[187] General Council, Incorporation of the Agreement on Electronic Commerce into Annex 4 of the WTO Agreement, WTO Doc. WT/GC/W/955 (2025).

soft in nature. For instance, Article 20 provides that "Assistance and support for capacity building should be provided to help developing and least-developed country Parties implement the provisions of this Agreement, in accordance with the nature and scope of such provisions."[188] As positive, one can view the many embedded flexibilities for developing and LDC parties. First, LDCs are fully excluded from dispute settlement with regard to any provisions for a period of seven years after the date of entry into force of the Agreement.[189] Second, developing and LDC parties can self-designate any provision of the Agreement for which they require an implementation period of no more than five years, with the possibility for a further extension.[190] Developed country parties, and developing country parties in a position to do so, are further "encouraged to provide developing and least-developed country Parties with support to conduct or update their needs assessment to identify gaps in capacity to implement this Agreement, either bilaterally or through relevant international organisations."[191] This is to be linked with targeted technical assistance and capacity building that address these specific needs; however, the provision is not binding.[192]

Beyond these few but positive developments, one can also note things that are key for economic development but are completely missing from digital trade agreements. One such thing is technology transfer. As Agarwal and Mishra argue, "[t]he rationale behind technology transfer is simple: for any meaningful progress, the have-nots need access to base technology and knowledge to sustain future efforts for an innovative, efficient, and competitive economy."[193] Missing are also meaningful provisions that go beyond digital inclusion and trade facilitation and take into consideration the broader implications of data-dependent economies and societies. In particular, one can think here of rules on data access and data sharing that will ensure that less developed countries can tap into data and develop their own digital and AI enterprises.[194] As another critical layer, very much in the context of this article, issues around human rights and sustainable development implications should also be considered. Developing countries and LDCs should be guided to ensure that purely commercial aspects do not dominate the regulatory environment for digital trade but contribute towards a balanced framework that takes into account

---

[188] World Trade Organization, Joint Statement on Electronic Commerce, art. 20.4, WTO Doc. INF/ECOM/87 (July 26, 2024).
[189] *Id.* art. 20.12.
[190] *Id.* arts. 20.6 and 20.7.
[191] *Id.* art. 20.8.
[192] *Id.* arts. 20.10 and 20.11. Article 20.11 outlines certain principles to be followed in the technical assistance and capacity building efforts.
[193] Agarwal & Mishra, *supra* note 9, at 283.
[194] *See, e.g.,* Burri II, *supra* note 9.

the economic as well as the non-economic dimensions of digital trade.

IV. CONCLUDING REMARKS

Digital trade law has developed exponentially in the last decade, especially when compared with other areas of international law. As observable from this article's discussion, the emergent governance framework is far-reaching and prescribes, in many situations, changes in domestic regulatory regimes that impinge on the policy space available to sovereign states to protect the fundamental rights of their citizenry and/or pursue distinct public policy objectives. Digital trade governance has also become more complex and increasingly covers a great number of, not strictly speaking, "trade", issues, while also directly addressing some human rights. This does not happen, however, in some systematic or coordinated manner and ultimately creates a false hierarchy of fundamental freedoms, with the right to privacy and personal data protection becoming overexposed, whereas others become marginalised. While this article could only offer a glimpse of the implications of burgeoning digital trade law for human rights, even against this somewhat limited backdrop, it appears essential that the discussions on these linkages ought to be intensified. As digital trade law evolves further, often behind closed doors with little to no transparency or multi-stakeholder participation, human rights lawyers should become more vigilant and grasp the impact of the technical digital trade provisions. Trade policymakers, too, should broaden their perspective and start paying attention to critical developments with human rights implications. At the same time, as this article revealed, there is also room for regulatory experimentation in the direction of more balanced rules, as the EU-led treaties and especially the new strand of digital economy agreements exemplify. Digital trade law, as any treaty-making is malleable and can provide a platform for more balanced, more sustainable rules that manage the trade-offs around data sovereignty and enable the growth of the data-driven economy while properly safeguarding human rights.