The (Potential) Impact of the Digital Economy Partnership Agreement on the Future of Cross-Border Personal Data Flows

Pablo TRIGO KRAMCSÁK, LL.M.
Ph.D. Researcher, Vrije Universiteit Brussel (VUB), Research Group on Law, Science, Technology & Society (LSTS); Researcher, Universidad de Chile, Faculty of Law, Centre for Information Technology Law Studies (CEDI).
ptrigo@derecho.uchile.cl

Michelle BORDACHAR BENOIT, LL.M.
Researcher, Universidad de Chile, Faculty of Law, Centre for Information Technology Law Studies (CEDI).
mbordachar@derecho.uchile.cl

Acknowledgments
This report was prepared with support from the Digital Trade Alliance. The authors would like to express gratitude to Dr. Jane Kelsey for her valuable input, insightful comments, and suggestions in the development of this report.

Table of Contents	
Summary	3
I. Introduction	5
II. DEPA: Background, Motivation, and Purposes	7
III. DEPA's Relevant Features: Open Character and Modular Design	8
IV. How Does DEPA Fit Into the New Trade Landscape?	11
V. Data Processing as a Core Issue for Digital Trade: Overview of the Different Regulatory Approaches to Cross-Border Data Flows	14
a. Data Realms	14
b. Key Aspects of the DEPA Parties' Cross-Border Data Flows Regulatory Frameworks	16
VI. DEPA's Approach to Cross-Border Data Flows	17
a. Personal Data Protection Provision	17
b. Cross-Border Data Flows Provision	19
c. Further Considerations in Relation to Other Global South Trade Agreements	21
d. Rules on Location of Computing Facilities	25
e. Use of Encryption	27
VII. DEPA and International Regulation of Artificial Intelligence. Background	29
a. Article 8.2. of DEPA. Analysis	30
VIII. Can the DEPA be Considered a Pathfinder for the Future Regulation of Cross-Border Data Flows, and What Effect Might this Have on the Regulatory Margin of Discretion that Countries Currently Have?	33
XI. Conclusions	35
References	37

Summary

Digital transformation stands as a pivotal catalyst for growth and innovation in today's global economy. The rapid expansion of digital markets, encompassing new business models, underscores the urgent need to establish appropriate trade regulations and governance mechanisms to address their complexities and challenges effectively.

There is no doubt that collecting, processing, and sharing personal data have become indispensable for the modern data-driven digital economy. Starting from the premise that global data flows underpin cross-border digital trade, there is an increasing consideration of the need to strengthen data governance to address current data protection and consumer privacy issues.

It is becoming increasingly common to find chapters on digital trade in new trade agreements. These digital trade chapters often include rules governing transborder data flows. In this sense, new plurilateral trade agreements are shaping the regulatory environment for digital data.

Asia-Pacific countries have adopted some of the most advanced and developed agreements focused on digital trade, such as the United States-Japan Digital Trade Agreement, the Singapore-Australia Digital Economy Agreement (SADEA), and the Digital Economy Partnership Agreement (DEPA). The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), for its part, contains an e-commerce chapter that applies to measures that "affect trade by electronic means" (a concept not defined), including provisions on personal information protection and cross-border transfer of information by electronic means, among others.

The DEPA, signed in 2020 among Chile, New Zealand, and Singapore, is one of the first comprehensive international agreements on digital commerce. During the negotiation process, Parties constantly referred to their intention to delineate an adequate framework for the progressive, reliable, and safe implementation of emerging technologies, including the governance of certain activities that underpin them, such as cross-border data transfers. It is to be noted that DEPA Parties envisioned this instrument as a model for possible World Trade Organization (WTO) e-commerce initiatives, as well as digital economy efforts within the Asia-Pacific Economic Cooperation (APEC) and other international bodies. Nonetheless, many DEPA provisions refer to non-binding commitments, starting points, or preliminary roadmaps for future collaboration. In this sense, it is worth asking: Does DEPA present a new approach to these issues, or does it reflect continuity with previous agreements?

Although the United States (US) did not participate in the negotiation process, DEPA contains language similar to the cross-border data provisions advanced by the US in the negotiations of what would eventually become the CPTPP. Among other relevant aspects, Parties strongly commit to facilitating the transfer of data across borders, even affirming the Parties' previous levels of commitment contained in other agreements. On this basis, it can be argued that this digital trade-focused agreement follows the US model on transborder data flows.

The purpose of this report is to analyze how the DEPA approach can shape or guide future negotiations and international governance rules on cross-border data flows and to determine whether DEPA provisions constrain governments from adopting their own standards on personal data transfers, identifying the possible added value of DEPA provisions.

Concerning the governance of personal data flows, DEPA's provisions do not introduce anything significantly new; they are essentially identical to those found in the CPTPP, initially proposed by the United States. This circumstance could be somehow related to DEPA's short negotiation period and countries' divergent views on personal data regulation, which 'inevitably required drawing heavily on existing agreements'.[1] In this sense, at least as far as cross-border data flows are concerned, DEPA does not represent a new path but rather the continuation of the one traced by the United States.

When contrasting specific provisions of the CPTPP with those found in the DEPA, there are some subtle differences. that seem to reveal the intention of DEPA signatories not only to maintain the commitments reached in the CPTPP but also to deepen data transfer obligations, setting some common ground on cross-border data standards. In this sense, DEPA seems to demand a more active involvement from the signatory countries to achieve the interoperability of their different legal approaches, for example, through a commitment to endeavor to mutually recognize the other parties' data protection trustmarks as a valid mechanism to facilitate cross-border information transfers. Nevertheless, while recognizing that DEPA's personal information protection provisions are more detailed than CPTPP rules, it must be concluded that they 'fail to set minimum standards'.[2]

In a global context where consensus remains elusive due to varying and, in some cases, conflicting approaches to essential digital trade issues, the fact that one of the earliest comprehensive international digital commerce agreements has adopted the US model does not seem innocuous. If we consider that DEPA has been specially conceived and designed as a pathfinder to 'influence and contribute to multilateral trade negotiations on digital trade',[3] by means of its flexible language and modular structure, it is not difficult to imagine that a wide accession and replication of its terms and provisions could end up producing a *de facto* harmonization under the US data governance model.

Additionally, this report will refer to how the DEPA has approached other emerging topics, in particular Artificial Intelligence governance, addressing, among other aspects, source code disclosure and access issues. In this regard, the real impact of the DEPA is notable for what it omits, i.e., commitments on non-disclosure of source code. Accordingly, it can be concluded that DEPA, unlike other new free trade or digital trade agreements, does not impose obstacles for parties to establish domestic measures in pursuit of algorithmic transparency, fairness, and accountability involving access to source codes or their algorithms.

[1] Kelsey, 2020.
[2] Ibid.
[3] Soprana, 2021: 168

I. Introduction

Digital trade plays a central role in today's world, opening the door 'to more countries, to small companies and startups, and to billions of individuals'.[4] According to the International Data Corporation (IDC), by 2022 over 65% of all global domestic product will be digitalized, driving over $6.8 trillion of direct digital transformation (DX) investment between 2020 and 2023.[5] This has led to a change in policymakers' approach toward digital trade, which 'has shifted from treating it largely as a traditional trade issue to recognizing its unique digital nature and tailoring the rules accordingly'.[6]

Although 'there is no single recognised and accepted definition of digital trade',[7] the terms "digital trade" and "e-commerce" are often used interchangeably'.[8] Nonetheless, it can be understood that the concept of digital trade, in a broad sense, is closely intertwined with the data-driven economy, i.e., with the datafication of trade and value chains (especially concerning the trade of services), a model that responds in some way to the fact that 'data circulation, storage and analysis are increasingly one of the central features of contemporary capitalism'.[9] In light of this, cross-border flows of digital data are 'core to all fast-evolving digital technologies, such as data analytics, artificial intelligence (AI), blockchain, Internet of Things (IoT), cloud computing and other Internet-based services',[10] enabling 'firms to use digital technologies to develop new markets'.[11]

Even with the growing relevance of this issue, at the multilateral level, the World Trade Organization (WTO) has failed to reach an international agreement to address the different aspects of digital trade in a comprehensive manner. In this context, it is becoming increasingly common to find chapters on digital trade in new trade agreements (that could be described as the 'resurgence of the spaghetti bowl of digital trade rules').[12] Such chapters often contain 'rules referring to the cross-border flow of data and rules banning or limiting data localization requirements'.[13] In the face of the failure of the WTO to reach a multilateral agreement on digital trade, preferential trade agreements are currently shaping 'the regulatory environment for digital data by overcoming some of the problems and inconsistencies of the multilateral regime',[14] effectively creating 'a new, albeit fragmented, governance framework for the data-driven economy'.[15]

Asia-Pacific countries have adopted some of the most advanced and developed agreements focused on digital trade, such as the United States-Japan Agreement on Digital Trade, the Singapore-Australia Digital Economy Agreement (SADEA), and the Digital Economy Partnership Agreement (DEPA).[16] The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), for its part, contains an e-commerce chapter that applies to measures that "affect trade by electronic means" (a concept not defined), including provisions on personal information protection and cross-border transfer of information by electronic means, among others.

---

[4] Manyika et al, 2016: i.
[5] Business Wire, 2020.
[6] Gao, 2018.
[7] OECD, n.d.
[8] Bacchus, 2021: 10.
[9] Peters, 2022: 5.
[10] UNCTAD, 2021: xv.
[11] Peters, 2022: 5.
[12] Agrawal and Mishra, 2022: 10.
[13] Burri, 2021a: 15.
[14] Burri, 2017: 408.
[15] Burri, 2021c: 78.
[16] On the other hand, it could be noted that the Regional Comprehensive Economic Partnership is taking a more cautious approach in this area.

The DEPA, adopted in 2020 between Chile, New Zealand, and Singapore, is one of the first comprehensive international agreements on electronic commerce.[17] It is 'not conceptualized as a purely trade agreement but one that is meant to address the broader issues of the digital economy',[18] given that DEPA's main objective is 'to establish basic rules to promote these countries as platforms for the digital economy'.[19]

DEPA Parties have highlighted that this agreement would contain 'new approaches' in digital trade issues, promoting 'interoperability between different regimes' and addressing 'the new issues brought about by digitalisation'.[20] Nevertheless, many DEPA provisions 'remain relatively tentative, with commitments for future work and consultation as the framework gets developed further'.[21] It is to be noted that the signatory states expressly considered that DEPA would support the WTO's e-commerce initiatives,[22] as well as digital economy efforts within the Asia-Pacific Economic Cooperation (APEC) and other international bodies. In this regard, this preferential agreement was negotiated with the aim of not only serving as a model for the regulation of new digital trade issues in the Asia Pacific region, but also with the 'belief that its individual provisions could end up being cut, pasted and tailored for inclusion in other international agreements, potentially including a WTO agreement'.[23]

This report aims to assess whether DEPA introduces a novel approach to cross-border personal data transfers or if it maintains consistency with prior agreements. Furthermore, it seeks to ascertain whether the international data flow regulations outlined in DEPA impose greater limitations on governments who seek to when establish new regulatory standards for personal data transfers. Based on the above, the following analysis seeks to answer the following main questions: Can the DEPA be considered a pathfinder for the future regulation of cross-border data flows? What is its "added value" in these matters? What vision or approach does DEPA reflect and promote in these matters?

In the field of transborder data flows regulation, this standalone digital trade agreement arguably mirrors the United States (US) model, thereby reaffirming the commitment levels established in prior agreements, including CPTPP. Although the United States did not participate in its negotiation process, DEPA follows the language advanced by the US in the negotiations of the Trans-Pacific Partnership.[24] The chapter on e-commerce '[d]espite the US having dropped out of the agreement with the start of the Trump administration [...] reflects the US efforts to secure obligations on digital trade and is a verbatim reiteration of the Transpacific Partnership (TPP) chapter'. This is evidenced in cross-border data flows issues, following an approach that promotes 'compatibility' between different data protection regimes, 'by essentially treating lower standards as equivalent', which implies prioritizing 'trade over privacy rights'.[25]

---

[17] Asia Trade Centre, 2020.
[18] Burri, 2021c: 91.
[19] Foreign Trade Information System of the OAS (SICE) (n.d.). *Digital Economy Partnership Agreement (DEPA), Background and Negotiations*. Available at: http://www.sice.oas.org/TPD/DEPA/DEPA_e.ASP
[20] Joint Ministerial Statement on the substantial conclusion of Digital Economy Partnership Agreement ("DEPA") negotiations. Available at: http://www.sice.oas.org/TPD/DEPA/Negotiations/DEPA_Jnt_Stmt_conclusion_e.pdf
[21] Asia Trade Centre, 2020.
[22] 'DEPA positions us to better shape and influence the progress of negotiations on digital trade issues in the WTO and elsewhere. The DEPA demonstrates to the WTO system what small states can do when they work together' (New Zealand Ministry of Foreign Affairs and Trade, 2020b).
[23] Bacchus, 2021: 7.
[24] Mention should also be made to the influence exerted by the Digital 2 Dozen (D2D) report, developed by the USTR during the TPP negotiations, which contains a 'set of rules and aims which is specifically drafted to be followed for the trade agreements related to open internet and digital economy', which include 'enabling cross-border data flows' (Heda, 2016).
[25] Burri, 2021d: 7.

II. DEPA: Background, Motivation, and Purposes

Chile, New Zealand, and Singapore (given their status of outward-facing and trade-dependent economies) are considered "like-minded" countries, presenting themselves (and being recognized) as strong promoters of free, open, and rules-based international trade.

These three economies initiated the negotiation process that would lead to which is considered the 'first free trade agreement linking Asia, the Pacific and the Americas',[26] i.e., the Trans-Pacific Strategic Economic Partnership, also known as P4,[27] that came into force in 2006. This agreement was negotiated with an open and broad vision, aimed at 'promoting the creation of a major strategic alliance for the liberalization of trade in the region', which means ' to create a platform for economic integration across the Asia Pacific',[28] also serving as a model for an eventual Asia-Pacific Economic Cooperation (APEC) Free Trade Agreement (Article 20.6 of the P4 agreement states that this agreement is open to accession 'by any APEC Economy or other State'). P4 is promoted by its supporters as a milestone for the Asia-Pacific region: the TPP negotiation process—which would culminate in the CPTPP—emerged from P4.[29]

In line with this same ethos, Chile, New Zealand, and Singapore launched on May 17, 2019, (on the sidelines of the 25th APEC Ministers Responsible for Trade Meeting) trilateral talks regarding an international agreement intended to set the regulatory contours of international digital trade, along with enabling the flourishing of new digital technologies.[30] While free trade agreements such as the CPTPP address certain aspects of digital trade (including, for instance, modern e-commerce rules in Chapter 14),[31] there is a prevailing recognition that 'new barriers arise and new international approaches are required'.[32] Consequently, this recognition has led to the formulation of standalone digital trade agreements..

Considering the role played by the P4 as the foundation of the CPTPP, Chile, New Zealand and Singapore have explicitly taken a "pathfinder" role in shaping regional trade rules, supported by their similarities as small trade-dependent countries that support open international trade policies. In this vein, these countries have also sought to engage actively in shaping the new cross-border digital markets rules, i.e., 'the forward-looking standards on digital trade',[33] in an effort to address emerging challenges presented by digitalization.

---

[26] New Zealand Ministry of Foreign Affairs and Trade, n.d.

[27] Negotiation of this agreement began in 2022 as Pacific 3 (P-3), involving New Zealand, Singapore and Chile, with Brunei Darussalam joining later (Undersecretariat of International Economic Relations of Chile (n.d.). *Acuerdos económico–comerciales vigentes, Chile-P4*. Available at: https://www.subrei.gob.cl/acuerdos-comerciales/acuerdos-comerciales-vigentes/p4

[28] Foreign Trade Information System of the OAS (SICE) (n.d.). *Comprehensive and Progressive Agreement for Trans Pacific Partnership Agreement (CPTPP) - Australia, Brunei Darussalam, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, and Vietnam, Background and Negotiations*. Available at: http://www.sice.oas.org/tpd/tpp/tpp_e.asp

[29] Petri and Plummer, 2020. 'A clue that a tiny FTA - P4 – changed into a significant trade agreement in the Asia-Pacific region was the US participation' (Yoshimatsu, 2014: 53).

[30] Asia Trade Centre, 2020.

[31] 'Data and digital trade chapters have been incorporated in regional agreements, such as the CPTPP, the Canada-United States- Mexico Agreement (CUSMA), and the Regional Comprehensive Economic Partnership (RCEP), and in stand-alone agreements, such as the US-Japan Digital Trade Agreement and Singapore's digital economy agreements (DEAs) with Australia, South Korea and the United Kingdom' (Fay and Ciuriak, 2022a: 2).

[32] Press release by The official website of the New Zealand Government, 18 May 2019, *NZ joins Chile and Singapore in talks on a Digital Economy Partnership*. Available at: https://www.beehive.govt.nz/release/nz-joins-chile-and-singapore-talks-digital-economy-partnership

[33] Press release by the Ministry of Trade and Industry of Singapore, 17 May 2019, *Singapore Leads The Way In New Digital Economy Partnership Agreement With Chile And New Zealand*. Available at:

While the CPTPP 'addressed e-commerce and digital trade issues as a sub-set of more comprehensive trade negotiations including intellectual property rights, technical barriers to trade, services, and rules of origin, DEPA Parties focused exclusively on negotiating disciplines on digital trade'.[34] It is understood that addressing these new issues is not 'a matter of simply transposing regulations developed for the tangibles economy to the intangibles economy',[35] most of which were originally designed 'with trade in goods in an analog world'.[36]

Drawing from the Joint Ministerial Statement on the launch of Digital Economy Partnership Agreement negotiations,[37] and press releases issued by the parties announcing the start of DEPA negotiations, the underpinnings of this process are as follows:

- business models and international trade have undergone a major transformation as a result of increasing digitalization (the new digital environment);
- the growth of digital trade has led to a lag in the development of relevant international trade rules and norms to better foster cross-border interoperability;
- there is a need for appropriate regulatory harmonization, which means creating new baseline digital trade rules applicable to emerging issues that impact the digital economy. In this regard, the DEPA would constitute a digital trade foundation, the first-of-its-kind and forward-looking agreement; and
- the DEPA is explicitly designed to complement and support the ongoing WTO negotiations on e-commerce, as well as digital economy work within APEC and other international fora.

DEPA negotiation concluded on January 21, 2020, after a short negotiation period.[38] Chile, New Zealand and Singapore signed the agreement on June 12, 2020, entering into force for Singapore and New Zealand on 7 January 2021, following the ratification of the agreement by both countries.[39] Finally, the DEPA entered into force for Chile on November 23, 2021.[40]

https://www.mti.gov.sg/Improving-Trade/Digital-Economy-Agreements/The-Digital-Economy-Partnership-Agreement

[34] Soprana, 2021: 151.

[35] Fay and Ciuriak, 2022a: 1.

[36] Garcia and Rebolledo, 2020.

[37] Available at: http://www.sice.oas.org/TPD/DEPA/Negotiations/DEPA_Jnt_Stmt_Launch_e.pdf

[38] 'The plan to sign a final agreement just six months later inevitably required drawing heavily on existing agreements. This included borrowing from the electronic commerce chapters in the Trans-Pacific Partnership (TPP) and Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)' (Kelsey, 2020).

[39] Press release by the Ministry of Trade and Industry of Singapore, 28 December 2020, *Digital Economy Partnership Agreement Enters Into Force*. Available at: https://www.mti.gov.sg/Newsroom/Press-Releases/2020/12/Digital-Economy-Partnership-Agreement-Enters-Into-Force

[40] Press release by the Undersecretariat of International Economic Relations of Chile, 23 November 2021, *El Acuerdo de Asociación de Economía Digital (DEPA) entra en vigor en Chile y sus miembros inician grupo de trabajo con China para evaluar su accesión al acuerdo*. Available at: https://www.subrei.gob.cl/sala-de-prensa/noticias/detalle-noticias/2021/11/23/el-acuerdo-de-asociación-de-econom%C3%ADa-digital-(depa)-entra-en-vigor-en-chile-y-sus-miembros-inician-grupo-de-trabajo-con-china-para-evaluar-su-accesión-al-acuerdo

III. DEPA's Relevant Features: Open Character and Modular Design

Various scholars characterize the DEPA as a 'stand-alone', '*sui generis* agreement',[41] or as a unique trade agreement,[42] emphasizing its distinct configuration. Additionally, DEPA is noted for its aspiration to broaden its membership,[43] being open to other WTO members who can meet its standards.[44] Consequently, this agreement would present a cross-regional spirit, which goes beyond the Asia-Pacific. DEPA is also described as 'a living agreement', one that is 'able to evolve as new technologies emerge, and new challenges arise'.[45] This adaptability is ensured through provisions enabling parties to amend the agreement when necessary, reflecting its responsiveness to the evolving digital landscape.[46]

Considering the above, it is argued that the DEPA stands out for its incremental approach, characterized by an innovative modular design.[47] It is argued that this agreement 'puts in place a set of legal building blocks that can be stacked up in different combinations', which allows future acceding parties 'to pick and choose which specific legal commitments on digital trade they are willing to assume'.[48] Notwithstanding that the agreement thematic modules 'are intended to work together',[49] DEPA structure also allows that its different blocks 'can be adopted and then slotted into other trade agreements'.[50]

DEPA is divided into various subject-specific modules, which cover a wide array of topics involved in the digital trade,[51] 'with three main objectives: facilitate seamless end-to-end digital trade; enable trusted data flows; and build trust in digital systems'.[52] Specific issues addressed are:

- business and trade facilitation (Module 2), including paperless trading (Article 2.2), domestic electronic transactions (Article 2.3), cross border logistics (Article 2.4), electronic invoicing (Article 2.5), trade of express shipments in electronic commerce (Article 2.6), and electronic payments (Article 2.7);
- treatment of digital products and related issues (Module 3), including customs duties on electronic transmissions (Article 3.2), non-discriminatory treatment of digital products (Article 3.3), and information and communication technology products that use cryptography (Article 3.4);
- data issues (Module 4), including personal information protection (Article 4.2), cross-border transfer of information by electronic means (Article 4.3), and location of computing facilities (Article 4.4);

[41] Soprana, 2021: 165.
[42] Burri, 2021d; Ramasubramanian, 2020.
[43] Fay and Ciuriak, 2022b.
[44] Press release by The official website of the New Zealand Government, 22 January 2020, *NZ concludes digital economy trade talks with Singapore and Chile.* Available at: https://www.beehive.govt.nz/release/nz-concludes-digital-economy-trade-talks-singapore-and-chile
[45] New Zealand Ministry of Foreign Affairs and Trade, 2020a.
[46] '[T]hrough the amendment procedure set in Article 16.3' (Soprana, 2021: 161).
[47] Ramasubramanian, 2020; Bacchus, 2021.
[48] Bacchus, 2021: 1.
[49] Honey, 2021: 3.
[50] Bacchus, 2021: 1.
[51] 'Although the agreement offers no further definition of 'trade in the digital economy', some scholars have observed that it reflects a wider conception of what constitutes 'digital trade' under other agreements' (Soprana, 2021: 153). Nevertheless, 'module 1, article 1.1.1 of the DEPA defines the scope of that agreement broadly as covering "measures adopted or maintained by a Party that affect trade in the digital economy."' (Bacchus, 2021: 10). 'Brought into the DEPA's focus are several digital economy topics that do not, at first blush, appear to be about trade. These issues include, for example, artificial intelligence, online safety, and open government data' (Honey, 2021: 4).
[52] Fay and Ciuriak, 2022b.

- wider trust environment (Module 5), including cybersecurity cooperation (Article 5.1), and online safety and security (Article 5.2);
- business and consumer trust (Module 6), including unsolicited commercial electronic messages (Article 6.2), online consumer protection (Article 6.3), and principles on access to and use of the Internet (Article 6.4);
- digital identities (Module 7);
- emerging trends and technologies (Module 8), including financial technology cooperation (Article 8.1), Artificial Intelligence (Article 8.2), government procurement (Article 8.3), and cooperation on competition policy (Article 8.4);
- innovation and the Digital Economy (Module 9), including public domain (Article 9.3), data innovation (Article 9.4), and open government data (Article 9.5).
- small and medium enterprises cooperation (Module 10);
- digital Inclusion (Module 11);
- transparency (Module 13); and
- dispute settlement (Module 14).

It is asserted that one of the main advantages offered by DEPA is the fact that it is 'made up of building blocks within a building block, resembling a multi-level complex adaptive system'.[53] This, in turn, allows new parties seeking access to the agreement to 'accept the different levels of commitments contained in each of these modules'.[54] DEPA specific design not only facilitates adaptation to diverse political and technical domestic contexts[55] but also underscores that for signatory parties the 'spread of DEPA is key',[56] encouraging the international multiplication of its modules.[57]

All these elements would make the DEPA stand out among other new-generation trade agreements, providing for greater flexibility and scalability. DEPA flexibility would be reinforced by the fact that 'many of its provisions are "soft law" rather than legally binding rules',[58] establishing, in different sections, soft obligations for the parties that 'do not directly require action from the members'.[59] In this sense, it is argued that many DEPA provisions 'remain relatively tentative' so that 'parties can be in compliance by simply endeavoring to comply'.[60] Also, it is alleged that DEPA provisions 'are simply to affirm existing obligations, share best practices, begin discussions and establish frameworks for future cooperation',[61] including the promotion of 'mutual recognition and acceptance of various norms and standards related to the digital economy'.[62]

It is worth noting that while DEPA's modular and flexible nature grants it the capacity to address a wide array of issues,[63] it may impede the attainment of the agreement's overarching objectives. This is because it could hinder the adoption of a holistic approach to the multifaceted challenges posed by the digital economy. In this sense, the configuration of the DEPA around separate and distinct modules, that are 'each whole unto themselves',[64] can make it challenging to reach comprehensive and consistent collective policies among the different (current and future) parties. It should also be also kept in mind that DEPA modules are

[53] Ramasubramanian, 2020.
[54] Bacchus, 2021: 7.
[55] Ramasubramanian, 2020.
[56] Asia Trade Centre, 2020
[57] Bacchus, 2021: 7.
[58] Honey, 2021: 2.
[59] Huld, 2021.
[60] Asia Trade Centre, 2020.
[61] Zhou, 2021.
[62] Huld, 2021.
[63] Burri, 2021c : 92
[64] Bacchus, 2021: 7.

separate but not equal, many of them containing soft law provisions, which may have an adverse effect on the real level of commitment of the participating countries, and ultimately on the potential impact and influence of this trade agreement.[65]

IV. How Does DEPA Fit Into the New Trade Landscape?

DEPA is promoted as 'a more up-to-date model for what digital trade agreements should look like',[66] being also seen as a 'template for new arrangements'[67] or 'a dialogue platform that can discuss digital issues and norm formation, reflecting the rapidly changing characteristics of the digital economy'.[68]

As discussed in earlier sections, DEPA parties were aware, right from the outset of the negotiation process, that this agreement would be a first-of-its-kind/digital-only deal ('prior to the DEPA, governments have grappled with setting digital trade rules through a patchwork of e-commerce provisions and chapters in FTAs'),[69] which meant that DEPA was 'designed to influence and contribute to multilateral trade negotiations on digital trade'.[70] In simpler terms, it was conceived as a 'forum expressly intended to influence how those issues will be addressed'.[71] For example, the DEPA's impact can be observed in 'another "digital only" deal', the SADEA, which 'mostly borrows the DEPA's modular approach'.[72]

It is also interesting to note that DEPA 'gives other countries the opportunity to join the agreement through a process of accession, whilst also providing for the opportunity of withdrawal'.[73] The first to be called upon to access the DEPA are the CPTPP signatory countries.[74] In this connection, on May 22, 2022, Canada 'submitted a formal request to launch negotiations for Canada's accession to the Digital Economy Partnership Agreement (DEPA)'.[75] In May 2023, on the sidelines of the 2023 APEC Ministers Responsible for Trade Meeting, in Detroit, Peru officially submitted a request for accession to DEPA.[76]

---

[65] Notwithstanding the foregoing, and as elaborated further below, some of the provisions, even if they are soft law, may have an impact on the way of interpreting other commitments undertaken by the parties.

[66] Aaronson, 2021.

[67] Xinzhen, 2022.

[68] Inha Jeonse University Gazette, 2022.

[69] Honey, 2021: 3.

[70] Soprana, 2021: 168.

[71] Fay and Ciuriak, 2022b.

[72] Bacchus, 2021: 8. Note that Australia and Singapore are co-convenors of the Joint Statement Initiative (JSI) on E-Commerce.

[73] Soprana, 2021: 152.
Keeping in mind that DEPA is open to other WTO members, interest in accessing the agreement extends beyond the Asia-Pacific region. See, for example, Joint Statement issued by representatives from 5 institutes and think-tanks are urging the UK government to access the DEPA (Available at: https://ifreetrade.org/pdfs/DEPA_JointStatement_Final1.pdf).

[74] Although the 'substantive content of the DEPA consists mostly of imported CPTPP measures' (Fay and Ciuriak, 2022a: 2).

[75] Press release by Global Affairs Canada, 22 May 2022, *Minister Ng announces Canada's request to join the Digital Economy Partnership Agreement*. Available at: https://www.canada.ca/en/global-affairs/news/2022/05/minister-ng-announces-canadas-request-to-join-the-digital-economy-partnership-agreement.html
It is considered that joining early to DEPA would allow Canada 'to participate in the development of governance of digital trade' (Fay and Ciuriak, 2022a: 2).

[76] Agencia Peruana de Noticias, 26 May 2023. *Peru submits request for adhesion to Digital Economy Partnership Agreement*. Available at: https://andina.pe/agencia/noticia-peru-submits-request-for-adhesion-to-digital-economy-partnership-agreement-941575.aspx

Nonetheless, it is possible to appreciate that DEPA has generated greater interest outside the CPTPP bloc. On September 13, 2021, South Korea (The Republic of Korea, abbreviated as ROK) officially notified New Zealand, depositary of the agreement, its intention to join the DEPA, after completing the domestic procedures to initiate negotiations on accession.[77] On 9 June 2023, the Ministers of Singapore, New Zealand, Chile, and the Republic of Korea announced 'the substantial conclusion of discussions on the ROK's accession to the DEPA'.[78] South Korea's formal accession to DEPA signifies a notable milestone, as it becomes the first non-founding member country to participate in the agreement. China's Ministry of Commerce (MOFCOM) filed on November 1, 2021, an application to join the DEPA,[79] formally notifying New Zealand 'of its intention to begin the process of accession to it'.[80] It is argued that 'joining the DEPA is in line with China's efforts to deepen reform and conduct a higher-level opening up',[81] showing Chinese 'willingness to be compatible with high-standard international digital rules'.[82] On the other hand, it is perceived that China's application to join DEPA 'is likely to renew interest among other potential participants about acceding to this agreement'[83] and could even 'broaden DEPA's role in developing international rules for digital economy'.[84]

It is plausible to maintain that DEPA 'is a step forward from several more limited plurilateral attempts'.[85] Moreover, it aspires to 'serve as the template for a much larger digital trade agreement, including possibly at the World Trade Organization itself'.[86] Certainly, as negotiations on the WTO Joint Statement Initiative (JSI) on electronic commerce negotiations are still underway,[87] 'the DEPA can be seen as an important step

[77] Press release by the Ministry of Trade, Industry and Energy (MOTIE) of South Korea, 13 September 2021, Korea initiates process to join Digital Economic Partnership Agreement (DEPA). Available at: http://english.motie.go.kr/en/pc/pressreleases/bbs/bbsView.do?bbs_cd_n=2&bbs_seq_n=870.
In its press release, the MOTIE recognizes DEPA's potential to 'serve as an extensive platform for the establishment of a digital cooperation network in the Asia-Pacific region'.

[78] Joint press release on the accession of the Republic of Korea to the Digital Economy Partnership Agreement, 9 June 2023. Available at: https://www.mti.gov.sg/Newsroom/Press-Releases/2023/06/Joint-Press-Release-on-the-accession-of-the-Republic-of-Korea

[79] Feifei, 2021.

[80] Press release by the Ministry of Foreign Affairs of Chile, 23 November 2021, *The Digital Economy Association Agreement (DEPA) enters into force in Chile and its members start a working group with China to evaluate its accession to the agreement*. Available at: https://www.minrel.gob.cl/news/the-digital-economy-association-agreement-depa-enters-into-force-in
It is argued that China's main motivation for applying to DEPA is to 'gain a seat at the table in a forum which could help shape global digital economy rules' (Zhou, 2021).

[81] Xinzhen, 2022.

[82] Nan, 2022.

[83] Asia Trade Centre, 2021.

[84] Nan, 2022. It is also worth mentioning that Costa Rica, in December 2022, requested to join DEPA (Ministerio de Comercio Exterior de Costa Rica, 23 December 2022, *Comunicado de Prensa CP-2829 Costa Rica solicita adhesión al Acuerdo de Asociación de Economía Digital*. Available at: https://www.comex.go.cr/sala-de-prensa/comunicados/2022/diciembre/cp-2829-costa-rica-solicita-adhesi%C3%B3n-al-acuerdo-de-asociaci%C3%B3n-de-econom%C3%ADa-digital/).

[85] Garcia and Rebolledo, 2020.

[86] Fay and Ciuriak, 2022b.

[87] On December 13, 2017, at the Eleventh Ministerial Conference (MC11) in Buenos Aires, 71 WTO members announced the JSI on electronic E-commerce, beginning exploratory work toward future WTO negotiations on trade-related aspects of electronic commerce. In February 2021, a total of 86 WTO members were formally participating in the e-commerce JSI negotiations. The topics covered by JSI E-commerce negotiations include electronic transaction frameworks, digital trade facilitation and logistics, cross-border data flows, customs duties on electronic transmissions, access to Internet and data, personal data protection, source code, and ICT products that use cryptography (Ismail, 2021: 1, 6, 10, 11). 'Given the diversity of the parties to the JSI, which differ widely in their economic and socio-political structures, economic interests, and perspectives on digital freedom, a JSI is unlikely to be sufficient to curb barriers to digital trade' (Hufbauer and Hogan, 2021: 2).

towards a broader multilateral agreement'.[88] Thus, for example, a WTO digital trade agreement could structure some potential obligations as optional 'in the same modular format as the DEPA and by drawing on the substantive obligations in the DEPA'.[89]

Nevertheless, it cannot be ignored that this agreement 'share[s] much in common with traditional trade agreements in both format and language'.[90] 'On the one hand, all rules of the CPTPP are replicated', as well as some rules contained in the United States-Mexico-Canada Agreement (USMCA), 'such as the one on open government data (but not source code)', and some US-Japan Digital Trade Agreement (DTA) provisions, 'such as the one on ICT goods using cryptography'.[91] In view of this, it is possible to state that '[o]verall, the DEPA is an ingenuine project'.[92]

For future accession processes, this factor—to replicate format and language contained in other agreements, especially the CPTPP—is far from being unproblematic. Notably, countries that are not signatories to the CPTPP may have reservations about adopting these provisions for various reasons. These reservations can stem from differences in both content and form, involving complex political, economic, and social considerations. This circumstance could affect the possibility that certain countries seeking to join DEPA accept all its modules. It should be noted DEPA provisions related to the governance of data flows (Article 4.3), "affirm" the parties' previous levels of commitment contained in other agreements. Among other effects, this would imply a reference to the commitments made by the three signatories to DEPA in the CPTPP (to which they are also a party). The situation described above certainly raises additional difficulties with accession of non-CPTPP parties to the DEPA.[93]

Likewise, the differences, particularities, and potential advantages offered by other regional agreements in matters related to digital trade must be considered, for example, allowing room for domestic regulation or emphasizing cooperation regarding some special issues. Here, it is worth briefly referring to the Regional Comprehensive Economic Partnership (RCEP), signed on November 2020 by the Association of Southeast Asian Nations (ASEAN) member states (Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand, and Vietnam) as well as Australia, China, Japan, New Zealand, and South Korea. Chapter 12 of the RCEP contains rules on digital trade and e-commerce, which provide an approach different from CPTPP regarding to the location of computing facilities, cross-border data transfers by electronic means, source code, and dispute settlement.[94]

It could be argued that RCEP's chapter 12 'is a good harbinger of the kind of agreement (should there be one) that we can expect from the JSI. This is because it showcases what China, the RCEP's dominant member state, is willing to accept in terms of e-commerce/digital trade provisions'.[95] In this connection, many of the RCEP provisions, for example, on localization requirements relating to computer facilities and cross-border data flows, would reflect China's vision and preferences in terms of digital commerce, framed within the concept of 'digital sovereignty',[96] providing 'a more recent insight into the China's positions'.[97]

[88] Soprana, 2021: 165.
[89] Bacchus, 2021: 16.
[90] Lovelock, 2020: 31.
[91] Burri, 2021c: 92.
[92] Burri, 2021c: 93.
[93] On the other hand, it can be understood that non-CPTPP parties accessing DEPA might not be affirming CPTPP rules on data flows. Instead, they could be affirming, for example, RCEP provisions (which some DEPA signatories are also party to). However, the reference to "previous" levels of commitment could make this interpretation difficult.
[94] Leblond, 2020. These provisions are 'subject to wide-ranging exceptions' (Jones et al., 2021: 12).
[95] Leblond, 2020.
[96] Bacchus, 2021: 31.
[97] Jones et al., 2021: 43.

V. Data Processing as a Core Issue for Digital Trade: Overview of the Different Regulatory Approaches to Cross-Border Personal Data Flows

a. Data Realms

Collecting and processing digital personal data have 'become indispensable for the business process'.[98] In today's global world, 'large amounts of data flows course through the internet, over borders and between individuals, firms and governments to power the internet and associated technologies',[99] leading to the development of a big data-driven digital economy, which encompasses 'all economic activities that use or are facilitated by digitized data'.[100]

Starting from the premise that global data flows underpin cross-border digital trade,[101] there is increasing consideration of the need to strengthen the international governance of digital data.[102] Given this, privacy and data protection issues 'have gained in the meantime importance and moved up on the negotiation agendas'.[103] Nevertheless, 'the inclusion of data governance as a trade-related issue complicates the policy process since it treats a critical yet complex policy matter'.[104] In this context, the possibility of solving data governance challenges is hampered by the fact that three main international actors, the United States, the European Union, and China, 'are creating three distinct data realms with different approaches to data governance'.[105] It's noteworthy that the US presents a sectoral approach that 'let business set the rules and to self regulate privacy',[106] while EU Member States 'ensure personal data protection under human rights law',[107] which finds expression in a comprehensive domestic regulation that grants strong protection to personal data, an approach that is not negotiable.[108] On the other hand, China has implemented stringent personal data protection regulations that tend to promote its own data-driven economy and internal security.[109]

Current rules governing cross-border data flows show two trends marked by the texts contained in the international agreements signed by the European Union and those signed by the United States, configurating

[98] Wang et al., 2021: 543.
[99] Aaronson, 2018.
[100] Chen, 2020: 1.
[101] Yakovleva and Irion, 2020a: 201.
[102] see e.g., ASEAN, 2017.
[103] Burri, 2021c: 80.
[104] Geist, 2018.
[105] Aaronson and Leblond, 2018: 1.
[106] Ibid. 'The US is characterized by its "permissive legal framework", which minimizes government regulation on the Internet and relies heavily on the self-regulation of companies' (Chin and Zhao, 2022: 10).
[107] Aaronson and Leblond, 2018: 15.
[108] EU-style cooperation pledges in ICTs and e-commerce contain broad agreements in these issues, 'except in the area of data protection' (Wunsch-Vincent and Hold, 2012: 205).
[109] Aaronson and Leblond, 2018: 19. These rules 'are mainly reflected in the "Cybersecurity Law", "Data Security Law", "Personal Information Protection Law", "Key Infrastructure Security Protection Regulations", "Cybersecurity Review Measures", and most recently in the "Measures for Data Export Security Assessment".' (Chin and Zhao, 2022: 18).
In this sense, it is argued that China's bid to join DEPA depends on clarification of its domestic data security laws, to 'negotiate carve-outs that allow it to maintain digital sovereignty' (Wong, 2022). It is possible to observe that a 'cornerstone of China's digital policy is the concept of cyber sovereignty', which includes, among other issues, imposing 'greater controls on international data flows' (Creemers, 2020: 3).

a new 'digital divide'.[110] While the European path recognizes the full autonomy of countries to determine their own rules when it comes to the protection of personal data–'[s]afeguarding a broad autonomy to maintain its data protection rules, including limitations on cross-border transfers of personal data'-,[111] i.e, 'balancing human rights and digital trade',[112] the United States approach emphasizes the need for facilitating the free flow of data across borders -'[i]n the US realm, policymakers have put few limits on cross-border data flows'.[113] On the flip side, we can observe the gradual emergence of the Chinese policy and model in these domains, 'closely tied with data sovereignty, national security and increasingly personal data protection to maintain the "legal, secure and free flows" of transborder data'.[114]

It is possible to argue, though, that since the adoption of the European Data Protection Directive in 1995, the EU has been setting 'the international agenda on specific data protection standards'.[115] The 1995 Data Protection Directive and its successor the General Data Protection Regulation (GDPR) 'have operated to promote data protection policies around the world and have had an extraordinary extraterritorial effect'.[116] In this regard, the EU 'promotes external data protection standards through the relatively coercive mechanism of the adequacy standard, decided on a case-by-case basis by the EU Commission'.[117] It is possible to speculate that 'this is a development caused by the so-called "Brussels effect," where the EU "exports" its own domestic standards by virtue of its large domestic market and regulatory capabilities and they become global'.[118]

As mentioned in previous sections, '[a]ttempts to multilateralize cross-border data flows within the WTO framework have failed so far', whereas 'the governance of cross-border data flows through trade agreements has become the mainstream trend'.[119] At this juncture, it is possible to observe a proliferation

[110] Chin and Zhao, 2022: 2.
[111] Yakovleva and Irion, 2020b: 14. 'From the perspective of the EU, unreservedly committing to free cross-border data flows likely collides with its approach of affording a high level of protection of personal data' as a fundamental right (Yakovleva and Irion, 2020a: 220). In this sense, the EU follows the principle that "the protection of personal data is non-negotiable" (Communication COM(2017)7 of 10 January 2017 from the Commission to the European Parliament and the Council. *Exchanging and Protecting Personal Data in a Globalised World*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A7%3AFIN). Along the same line, the EU's approach is 'to promote its data protection values and facilitate data flows by encouraging convergence of legal systems' (ibid.). This implies convergence with EU's level of data protection, including its personal data protection principles. To foster convergence, it would be necessary to develop 'high and interoperable personal data protection standards globally. This contributes to the more effective protection of individuals' rights and at the same time reduces obstacles to the cross-border flow of data as an important element of free trade' (ibid.).
[112] Chin and Zhao, 2022: 3.
[113] Aaronson and Leblond, 2018: 3. 'US Internet companies have significant and irreplaceable competitive advantages in the global market competition; therefore, the free flows of data or information has become a basic principle of US trade agreements'. Accordingly, the US 'has always emphasized export orientation, advocated the opening of the digital market, and advocated the free flows of data (Chin and Zhao, 2022: 18).
In this way, the US promotes the concept of 'interoperability', linked to the idea of 'mutual recognition' of different privacy models, which differs from the EU's notion of 'convergence' of regulatory frameworks. The US concept of interoperability aims at reducing data transfer formalities through cross-recognition of different standards and mechanisms. This would imply the risk of recognizing as equivalent diverging standards (with 'fundamental differences'), including much lower standards of data protection, e.g., mere voluntary commitments. (See Greenleaf, 2013; Greenleaf and Waters, 2012).
[114] Chin and Zhao, 2022: 6.
[115] Reidenberg, 2000: 1367.
[116] Bennett, 2020 : 1.
[117] Ibid.
[118] Burri, 2021e: 78.
[119] Chin and Zhao, 2022: 2.

of the 'US led digital trade template' on the free flow of data, introduced in the CPTPP, USMCA, and the United States-Japan Digital Trade Agreement.[120]

b. Key Aspects of the DEPA Parties' Cross-Border Data Flows Regulatory Frameworks

In consideration of this backdrop, it is pertinent to provide an overview of certain salient dimensions within the regulatory frameworks pertaining to cross-border data flows among original signatories to DEPA.

First, it is noteworthy that none of the initial signatories of the DEPA is part of Convention 108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data,[121] 'the only binding international convention within the international privacy and data protection policy space'.[122]

Secondly, the three original members of the agreement are members of APEC and, as such, they endorsed in 2004 the APEC's Privacy Framework. The purpose of this model framework is—through a set of non-binding principles and implementation guidelines—to promote a flexible approach to information privacy protection across APEC member economies, in order to avoid barriers to information flows and ensure continued trade.[123] However, this framework 'do[es] not have any legal status and [is]are best seen as agreed aspirations, supported by consensus-based commitments to cooperate'.[124] In addition, its principles are considered to be 'unnecessarily weak', with 'no meaningful enforcement requirements'.[125] 'In 2011, Cross-Border Privacy Rules (CBPR) were announced as a mechanism to bring increased certainty to the APEC Privacy Framework's transfer rules'.[126] The CBPR is a voluntary regime designed as a code of conduct model 'that businesses can be certified as conforming to, to demonstrate that they have implemented protections consistent with the APEC Privacy Framework for the purpose of acting as personal data transfer recipients'.[127] Among original DEPA Parties, Singapore is the only one to meaningfully participate in the CBPR scheme, operationalizing the system through the appointment of 'Assessment Bodies' ('Accountability Agents' in APEC jargon), to assess whether companies are CBPRs compliant'.[128]

For a more comprehensive grasp of the disparities in cross-border data flow standards among the founding members of DEPA, it is useful to refer to the Digital Economy Report 2021, 'Cross-border data flows and development: For whom the data flow', prepared by the United Nations Conference on Trade and Development (UNCTAD). This report contains a mapping of different national regulations regarding cross-border data flows, classifying them into different approaches or 'level of restrictiveness'. In this regard, the document notes that Singapore would be more or less aligned with a 'light-touch approach', implying that 'all data, including personal data, can generally flow freely across borders with minimal regulatory

[120] Yakovleva and Irion, 2020a: 220.
[121] However, New Zealand Privacy Commission and Chile's Council for the Transparency (independent public agency responsible for monitoring that public entities comply with the Chilean data protection law) are observers on Convention 108 Consultative Committee.
[122] Bennett, 2020: 1.
[123] See https://www.apec.org/publications/2005/12/apec-privacy-framework
[124] de Hert and Papakonstantinou, 2015: 13.
[125] Greenleaf, 2009: 1.
[126] Phillips, 2018: 576.
[127] Ibid.
[128] Greenleaf, 2020: 6.

requirements (if any)'.[129] New Zealand, meanwhile, is considered a country with a 'prescriptive approach', 'that impose soft or intermediate conditional requirements for cross-border data flows'.[130]

VI. DEPA's Approach to Cross-Border Data Flows

In the domain of cross-border data flows, DEPA closely aligns with the approach championed by the United States during the TPP negotiations. This alignment extends to various dimensions such as personal data protection, requirements for cross-border transfer of information, or the location of computing facilities where this information is processed and stored. It's important to note that even though the United States is not a participant in the CPTPP, its provisions draw heavily from the TPP, where the US played a significant role in shaping the negotiation process. Of particular significance are the 2015 United States Digital Trade Negotiating Objectives, established by the US Congress. These objectives encompass preventing forced localization requirements, removing constraints on digital trade and data flows, and ensuring that relevant legitimate regulations are as least trade restrictive as possible.[131]

a. Personal Data Protection Provision

Concerning personal information protection, it is possible to note that DEPA Article 4.2 takes as its basis the text of CPTPP Article 14.8, to which it incorporates some new elements that seem to reveal an intention not only to maintain the commitments reached in the CPTPP, but also to deepen data transfer obligations.

Below, in the Box 1, it is possible to see these changes in more detail. We have marked in italics the words that have been modified and in bold the new text that was not in the CPTPP.

Box 1

Article 4.2: Personal Information Protection

1. The Parties recognise the economic and social benefits of protecting the personal information of *participants in the digital economy and the importance of such protection* in enhancing confidence in *the digital economy* **and development of trade.**

2. To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce *and digital trade*. In the development of its legal framework for the protection of personal information, each Party *shall* take into account principles and guidelines of relevant international bodies.11

3. The Parties recognise that the principles underpinning a robust legal framework for the protection of personal information should include: (a) collection limitation; (b) data quality; (c) purpose specification; (d) use limitation; (e) security safeguards; (f) transparency; (g) individual participation; and (h) accountability.

4. Each Party *shall adopt* non-discriminatory practices in protecting users of electronic commerce from personal information protection violations occurring within its jurisdiction.

[129] UNCTAD, 2021: 135.

[130] UNCTAD, 2021: 136. Chile is not classified under these parameters, but since its general regulation on the protection of personal data (Law No. 19.628 on Protection of private life) does not contain any specific provisions regarding cross-border data flows, it could be concluded that it has an 'light-touch approach'.
It should be noted that New Zealand stands out for being the only one of these three countries that meets the high European Union personal data protection standards. In 2012 the European Commission formally ruled that New Zealand's privacy law ensures 'an adequate level of protection for personal data transferred from the Union' (European Commission, n.d.).

[131] Congressional Research Service, 2021: 13.

5. Each Party *shall* publish information on the personal information protections it provides to users of electronic commerce, including how: (a) individuals can pursue remedies; and (b) businesses can comply with any legal requirements.

6. Recognising that the Parties may take different legal approaches to protecting personal information, each Party *shall pursue* the development of mechanisms to promote compatibility **and interoperability** between their different regimes **for protecting personal information**. These mechanisms may include:

(a) the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement;

(b) broader international frameworks;

(c) where practicable, appropriate recognition of comparable protection afforded by their respective legal frameworks' national trustmark or certification frameworks; or

(d) other avenues of transfer of personal information between the Parties.

7. The Parties *shall exchange* information *on how* the mechanisms in paragraph 6 *are applied in their respective jurisdictions* and explore ways to extend these or other suitable arrangements to promote compatibility **and interoperability** between them.

8. The Parties shall encourage adoption of data protection trustmarks by businesses that would help verify conformance to personal data protection standards and best practices.

9. The Parties shall exchange information on and share experiences on the use of data protection trustmarks.

10. The Parties shall endeavour to mutually recognise the other Parties' data protection trustmarks as a valid mechanism to facilitate cross-border information transfers while protecting personal information.

Footnote 11 provides that "[f]or greater certainty, 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 data protection or privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to data protection or privacy".

The text of DEPA Article 4.2, paragraphs 1, 2, 4, 5, and 7 closely mirrors that of the CPTPP, with only slight alterations. These modifications primarily involve changes in the governing verbs and the introduction of the concept of "interoperability", which is a distinctive feature of the US model.[132] Another subtle but interesting change is the modification of verb tenses. Meanwhile in CPTPP (Article 14.8, paragraph 5) Parties "should encourage" the development of mechanisms to promote compatibility between the different regimes, in DEPA (Article 4.2, paragraph 6) each Party "shall pursue" the development of such mechanisms to promote not only compatibility between the different regimes, but also interoperability.[133]

Among the most substantive changes is the text of the third paragraph, relating to the principles governing the processing of personal data, and the incorporation of three new paragraphs at the end of the provision.

[132] As opposed to the concept of "convergence", promoted by the European Union model.

[133] Other changes involve the replacement of the expressions "users of electronic commerce" by "participants of digital trade"; the elimination of any reference to "consumers"; and the addition of two new subparagraphs to the list of possible mechanisms to promote compatibility between different data protection regimes ("where practicable, appropriate recognition of comparable protection afforded by their respective legal frameworks' national trustmark or certification frameworks;" and "other avenues of transfer of personal information between the Parties". Meanwhile in CPTPP, to this end, the Parties "shall endeavour to exchange" information on any such mechanisms, in DEPA the agreement of the parties is not to "endeavour to exchange" information, but directly to exchange it).

In paragraph 3, the Parties establish which principles they consider the basis for processing personal data. This might seem to be a step forward in terms of personal data protection as it would develop a common ground of minimums; however, the principles indicated therein are none other than the first-generation principles included in the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980. The core of the Guidelines is the eight 'basic principles of national application', which, since the 1990s, have been considered inadequate for providing 'sufficient privacy regulation' in an Internet-driven world.[134] Therefore, without elaborating on their content, the mere mention of a set of non-updated principles might not be sufficient to establish a minimum threshold.

In the last three paragraphs, the Parties declare their intention to encourage the adoption of data protection trustmarks by businesses; to exchange information on the use of such trustmarks; and to endeavour to mutually recognise the other Parties' data protection trustmarks as a valid mechanism to facilitate cross-border information transfers. In this sense, DEPA strongly promotes the adoption of voluntary self-regulatory approaches, which could be considered, based on what is indicated in footnote 11, in some way equivalent to the implementation of comprehensive or sectoral privacy/data protection laws.

While these paragraphs do not require direct action by the Parties, their inclusion could have practical effects. Take, for instance, paragraph 10, which does not oblige Parties to mutually recognise the other Parties' data protection trustmarks as a valid mechanism to facilitate cross-border information transfers. In this respect, the implications of the commitment to "endeavour to mutually recognise the other Parties' data protection trustmarks as a valid mechanism to facilitate cross-border information transfers while protecting personal information" may be challenging to discern, particularly when dealing with trustmarks that dare not fully compatible with a DEPA Party's regulatory approach or privacy and personal data processing standards.

Given the premise outlined above, it becomes reasonable to anticipate mutual recognition, at least among the current DEPA Parties (and potentially among future APEC members joining DEPA), for the APEC CBPR certification scheme.

b. Cross-Border Data Flows Provision

Regarding the rules governing cross-border data flows, DEPA Article 4.3 (see box 2 below) takes verbatim CPTPP Article 14.11. This implies that DEPA, such as the CPTPP, 'explicitly formulates a commitment to the free flow of personal data across borders'.[135] Additionally, Article 4.3 of the DEPA includes exceptions modelled on GATS Article XIV on General Exceptions[136]. However, an interesting change in CPTPP, followed by DEPA, is that it abandons the reference to the "necessity" as an element to be considered to determine whether a measure is justifiable under the terms of the provision, and instead states that the measures should "not impose restrictions on transfers of information greater than are required to achieve the objective". In this regard, it has been argued that the difference would be purely semantic, and that according to the WTO Secretariat, 'is yet another way to convey the concept of "necessity"'. [137] Other authors argue that this language sets a different bar than the term "necessary" and 'makes the relevance of WTO jurisprudence regarding the term "necessary" doubtful'.[138]

[134] Greenleaf, 2019: 5.
[135] Naef, 2022: 377.
[136] Mattoo and Meltzer, 2019: 784. Nevertheless, CPTPP cross-border data flows commitments 'cover all information flows and, unlike the GATS, are not limited to data flows necessary for the provision of cross-border services' (Ibid.).
[137] Yakovleva, 2020: 491.
[138] López, Condon & Muñoz, 2021: 223.

Moreover, DEPA, by following the CPTPP model, differs from the GATS rules regarding another aspect: the measure must achieve a "legitimate public policy objective". While there is a list of public policy objectives in GATS, 'the CPTPP provides no such enumeration and simply speaks of a 'legitimate public policy objective'.[139] This is 'a novel phrase in international trade law on which there is no jurisprudence'.[140] While it could be estimated that this term 'permits more regulatory autonomy', the parties 'may be linked however to legal uncertainty'[141] ('what counts as 'legitimate' is not self-judging').[142]

Given the aforementioned considerations, a question that naturally arises is when a measure could be understood as imposing restrictions "greater than are required". If we relate this question to what was pointed out on data protection trustmarks in the preceding section, it becomes reasonable to inquire about the likelihood of restrictions stemming from a measure that extends beyond trustmarks requirements being deemed "greater than required to achieve a legitimate public policy objective". In other words, based on what is stated in footnote 11, there's a potential to question whether those measures that are not just voluntary ("voluntary undertakings by enterprises") are more restrictive than required to achieve the objective. Consequently, such a perspective lends would support to the argument that voluntary self-regulatory approaches may entail fewer burdens in the pursuit of a legitimate public policy objective.

Considering that all DEPA Parties are also APEC members, it becomes pertinent to assess whether the APEC CBPR certification system could serve as "a valid mechanism to facilitate cross-border information transfers while protecting personal information", and thereby, whether any additional requirements, exceeding those mandated the APEC Privacy Framework, might be considered as imposing restrictions greater than required. The APEC framework has been heavily criticized, among other issues, for being based on 'unnecessarily weak' privacy principles and lacking effective enforcement.[143] However, it should be kept in mind that APEC Privacy Framework principles correspond to those expressly enshrined in paragraph 3 of Article 4.2 DEPA.

Below, in the Box 2, is the text of DEPA Article 4.3. The only difference between this provision and CPTPP Article 14.11 is the addition of a new sentence at the beginning, whereby the parties state that they affirm their level of commitment relating to the cross-border transfer of information (text marked in bold[144]). It should be noted that, among other effects, this language would imply a reference to the commitments made by the three signatories to DEPA in the CPTPP (to which they are also a party).

Box 2

Article 4.3: Cross-Border Transfer of Information by Electronic Means.

The Parties affirm their level of commitments relating to cross-border transfer of information by electronic means, in particular, but not exclusively:

[139] Burri, 2021c: 86.
[140] Waitangi Tribunal, 2023: 128. Jane Kelsey points out that '[a]s the 'legitimate public policy objective' provision is not incorporated from the WTO, there is no direct requirement to consider WTO jurisprudence' (Waitangi Tribunal, 2023: 130).
[141] Burri, 2021c: 86.
[142] Waitangi Tribunal, 2023: 129. To illustrate this point, Jane Kelsey refers precisely to privacy regulations: 'the European Union's (EU) attempt to clarify the term 'legitimate public policy objective' as including 'the protection of privacy' in the 'stocktake text' for the ongoing WTO plurilateral negotiations on e-commerce. This, she said, shows the EU was not 'convinced that privacy protection would be accepted as a legitimate public policy objective and so again we've got this problem about uncertainty' (Ibid.).
[143] Greenleaf, 2009: 1.
[144] In this case, the text that appears in italics here also appears in italics in the commercial agreement.

1. The Parties recognise that each Party may have its own regulatory requirements concerning the transfer of information by electronic means.

2. Each 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.

3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:

(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and

(b) does not impose restrictions on transfers of information greater than are required to achieve the objective.[145]

In contrast, it is noteworthy to keep in mind RCEP provisions on cross-border data flows, as they provide more autonomy and flexibility to its signatories. Parties agree, in Article 12.15 RCEP, "not to prevent" cross-border transfers, but 'inconsistent' measures are allowed if they are "necessary" in order to achieve a "legitimate public policy objective". Nevertheless, unlike US-style agreements, 'there is no requirement that the measure be "least burdensome" to achieve the objective. In addition, the obligations are subject to a completely self-judging and non-disputable national security exception'.[146] In RCEP footnote (14), the parties affirm that "the necessity behind the implementation of such legitimate public policy shall be decided by the implementing Party".

[145] In his article "Data Rules In Modern Trade Agreements", Michael Geist points out that there are four requirements that must be met in order for the CPTPP's general exception to be applicable. Therefore, it could be argued that Article 14.11 CPTPP establishes a multi-tiered test that would make it possible to challenge the consistency of a measure restricting the cross-border transfer of information by electronic means, with the conditions of the exception based on the following considerations:

i. on the ground that the public policy objective is not legitimate.

ii. on the ground that the measures are being applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination

iii. on the ground that the measures are being applied in a manner which would constitute a disguised restriction on trade; and

iv. on the ground that the measures applied impose restrictions on transfers of information greater than are required to achieve the objective.

Then, 'the benefits of the general exception may be illusory since the requirements are so complex (each aspect must be met) that countries have rarely managed to meet the necessary conditions. For countries concerned about the weakened privacy protections, the trade agreement restriction on the use of data localization requirements may pose an insurmountable barrier' (Geist, 2018).

[146] Jones et al., 2021: 22. Note that this provision is not subject to the dispute settlement chapter (article 12.17.3 RCEP).

c. Further Considerations in Relation to Other Global South Trade Agreements

When comparing the DEPA standards analyzed above with other agreements signed in the global south—and in which one DEPA signatory, Chile, has participated—it is possible to appreciate some differences that seem relevant to us.

1. Chapter 8 on Electronic Commerce of the Chile-Uruguay Free Trade Agreement

Box 3

Article 8.7. Protection of Personal Information

1. The Parties recognize the benefits of protecting the personal information of users of electronic commerce and the contribution this makes to enhancing consumer confidence in electronic commerce.

2. The Parties shall adopt or maintain laws, regulations or administrative measures for the protection of personal information of users engaged in electronic commerce. The Parties shall take into consideration existing international standards in this area, as provided for in Article 8.2.5 (f).

3. Each Party should publish information about the protection of personal information it provides to users of electronic commerce, including how:

(a) Individuals can exercise resources, and

(b) Companies can comply with any legal requirement.

4. The Parties should exchange information and experiences regarding their personal information protection legislation.

5. The Parties shall encourage the use of mechanisms for encrypting users' personal information, and their dissociation, in cases where such data are provided to third parties, in accordance with applicable legislation.

Article 8.10. Cross-border Transfer of Information by Electronic Means

1. Each Party shall permit the cross-border transfer of information by electronic means, including personal information, where this activity is for the conduct of the business of a person of a Party.

2. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 1 to achieve a legitimate public policy objective, provided that the measure is not applied in a manner that would constitute a means of arbitrary or unjustifiable discrimination, or a disguised restriction on trade. The Parties recognize that each Party may have in its regulatory framework its own regulatory requirements for the transfer of information by electronic means.[147]

The Free Trade Agreement between the Republic of Chile and the Oriental Republic of Uruguay (Chile-Uruguay FTA) was signed in October 2016. This agreement was put in place before the DEPA negotiation process began, and its initial round of negotiations commenced on February 23, 2016, shortly after the signing of the TPP.[148] This situation highlights that Chile's stance on cross-border personal data flows in the trans-Pacific context differs somewhat from its approach within the South American region. Regarding

[147] https://edit.wti.org/document/show/d1cba00f-4306-48a6-843d-c9a4bdcf7a93
[148] http://www.sice.oas.org/TPD/CHL_URY/Negotiations/1st_round_neg_s.pdf

the protection of personal data, it is stated that parties 'shall adopt or maintain laws, regulations or administrative measures for the protection of personal information', without mentioning voluntary trustmarks as an equivalent measure.[149] Unlike the DEPA, this FTA does not actively promote the mutual recognition of data protection trustmarks as a valid mechanism for the cross-border flow of data, nor does it recognize self-regulatory approaches as equivalent to comprehensive or sectoral data protection laws.

Additionally, Article 8.2, Scope and General Provisions, states in number 5 that '[c]onsidering the potential of electronic commerce as a tool for social and economic development, the Parties recognize the importance of [...] (f) To guarantee the security of e-commerce users, as well as their right to personal data protection'. In this regard, footnote (3) establishes that '[t]he Parties will understand for greater certainty that the collection, processing and storage of personal data will be carried out following the general principles of prior consent, legitimacy, purpose, proportionality, quality, security, responsibility and information'. In this sense, the Chile-Uruguay FTA text expressly recognises individuals' right to personal data protection, together with referring, beyond the "remedies", to the exercise of resources by individuals to safeguard this right.

As for cross-border data transfer measures and the recognition of domestic regulatory frameworks**,** the Chile-Uruguay FTA text aligns closely with that of DEPA. Similar to both CPTPP and DEPA, the agreement stipulates that measures limiting cross-border data flows must serve a "legitimate public policy objective". However, Chile-Uruguay FTA presents an important difference: instead of including a rule of subjective consideration ("does not impose restrictions on transfers of information greater than are required to achieve the objective"), it was decided to expressly and broadly recognize that "each Party may have in its regulatory framework its own regulatory requirements for the transfer of information by electronic means". This is particularly noteworthy, considering that the phrase "greater than are required" could be used to challenge a higher standard of protection.

Lastly, it should be noted that the Chile-Uruguay FTA encourages 'the use of encryption or security mechanisms for the personal information of the users, and their dissociation or anonymization, in cases where said data is provided to third parties'.[150]

2. Chapter 11 on Electronic Commerce of the Chile-Argentina FTA

Box 4

Article 11.5. Personal Data Protection

1. The Parties recognize the benefits of protecting the personal information of users of electronic commerce and the contribution this makes to enhancing consumer confidence in electronic commerce.

2. The Parties shall adopt or maintain laws, regulations, or administrative measures for the protection of personal information of users engaged in electronic commerce. The Parties shall take into consideration existing international standards in this area, as provided in subparagraph (f) of Article 11.2.5.

3. Each Party shall make efforts to ensure that its legal system relating to the protection of personal information of users of electronic commerce is applied in a non-discriminatory manner.

[149] This despite the fact that in Article 8.2.5(b) the Parties recognize the importance of encouraging 'self-regulation in the private sector to promote confidence in e-commerce, taking into account the interests of users, through initiatives such as industry guidelines, model contracts, codes of conduct and trust seals'.
[150] Burri, 2021b: 31. See also Article 10.8(6) Brazil-Chile FTA.

4. Each Party shall endeavor to publish information on the protection of personal information it provides to users of electronic commerce, including how:

(a) Individuals may exercise recourse, and

(b) Companies can comply with any legal requirement.

5. The Parties shall exchange information and experiences regarding their personal information protection legislation.

6. The Parties shall encourage the use of security mechanisms for the personal information of users, and its dissociation, in cases where such data is provided to third parties, in accordance with their legal system.

7 The Parties undertake to apply to the personal data they receive from the other Party a level of protection at least similar to that applicable in the jurisdiction of the Party from which the data originate, through mutual agreements, general or specific, or in broader international frameworks, admitting for the private sector the implementation of contracts or self-regulation.[151]

Article 11.6. Cross-border Transfer of Information by Electronic Means

1. The Parties recognize that each Party may have its own regulatory requirements on the transfer of information by electronic means.

2. Each Party shall permit the cross-border transfer of information by electronic means, where such activity is for the conduct of the business of a person of a Party (2) .

3. The Parties may establish restrictions on the cross-border transfer of information by electronic means to achieve a legitimate public policy objective, provided that the measure is not applied in a manner that would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade.

_____

Footnote (2) provides that "[f]or greater certainty, this paragraph shall be subject to compliance with the provisions of Article 11.5.7".[152]

In the area of personal information and data transfers, the Free Trade Agreement between the Republic of Argentina and the Republic of Chile (Chile-Argentina FTA), signed in November 2017, follows in its Electronic Commerce Chapter a similar path to the Chile-Uruguay FTA, including the express recognition of individuals' right to personal data protection and a list (in Article 11.2.5(f) footnote (1)) of principles to be followed in the Parties' data protection laws ('prior consent, legitimacy, purpose, proportionality, quality, security, accountability and information'). Furthermore, the agreement encouraging 'the use of security mechanisms for the personal information of users, and its dissociation, in cases where such data is provided to third parties'.

Besides, it is important to stress that Chile-Argentina FTA incorporates a provision that aims in more concrete terms to establish a minimum threshold in personal data protection standards, requiring the parties to apply a level of protection to the transferred personal data at least similar to that applicable in the

[151] The English translation of the Chile-Argentina FTA, provided by Electronic Database of Investment Treaties (EDIT) and available at https://edit.wti.org/app.php/document/show/bf9aa665-cb2a-472f-849d-090e28b096fb, is missing the introductory words of the Article 11.5.7, stating that "The Parties undertake to apply to the personal data they receive [...]".

[152] https://edit.wti.org/document/show/bf9aa665-cb2a-472f-849d-090e28b096fb

transferring country. Regarding cross-border transfer of information by electronic means, Article 11.6.2 indicates that '[e]ach Party shall permit the cross-border transfer of information by electronic means, where such activity is for the conduct of the business of a person of a Party'. Subsequently, footnote (3) points out that '[f]or greater certainty, this paragraph shall be subject to compliance with the provisions of Article 11.5.7'. This specific provision establishes that '[t]he Parties undertake to apply to personal data received from the other Party a level of protection at least similar to that applicable in the jurisdiction of the Party from which the data originates, through mutual agreements, general or specific, or in broader international frameworks, admitting for the private sector the implementation of contracts or self-regulation'.

In summary, this bilateral FTAs, signed prior to the launch of the DEPA negotiation process, shows that at the regional level, Chile was following a different path compared to its transpacific approach, aimed at achieving regulatory convergence in the area of data privacy, built on laws or administrative measures for the protection of personal information of users engaged in electronic commerce, ensuring that they benefit from a level of safeguard at least similar to the legal and administrative provisions in force in the exporter country.

However, it's important to note that the level of commitments on the protection of personal information transferred across borders reached in the Chile-Argentina FTA was not fully replicated in the Chile-Brazil FTA, signed in November 2018 (before the launch of the DEPA negotiation process), especially in terms of promoting regulatory convergence in the levels of protection to personal data. On the other hand, chapter 10 of the Chile-Brazil FTA, on Electronic Commerce, while acknowledging the need for guaranteeing electronic commerce users' "right to the protection of personal data" (Article 10.2.5(f)),[153] does not mention the basic principles applicable to the collection, processing, and storage of personal data.[154]

d. Rules on Location of Computing Facilities

As regards the rules on location of computing facilities, similar to the case of Article 4.3 on the Cross-Border Transfer of Information, DEPA Article 4.4 is almost identical to Article 14.13 CPTPP, with the sole exception of the addition of a new sentence at the beginning (refer to Box 5 below).

Box 5

Article 4.4: Location of Computing Facilities

The Parties affirm their level of commitments relating to location of computing facilities, in particular, but not exclusively:

"1. The Parties recognise that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications.

2. No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.

3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:

[153] https://edit.wti.org/document/show/e62cfb4c-abbf-43d9-ae34-a15c7d057ab4

[154] This can be explained by the fact that at the time this agreement was negotiated, Brazil did not have a personal data protection law.

(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and

(b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective."

The provided DEPA text includes new additions marked in bold, which were not present in the CPTPP. In this case, the text that appears in italics here also appears in italics in the agreement.

Article 4.4 of the DEPA includes a general restriction on data localization of computing facilities. Although there is no precise definition of what constitutes a data localization measure, in a strict sense, it can be understood as a requirement that the data generated in a country be stored on a server or other storage device located within that country' imposed for different purposes, including security and, often, protectionist reasons.[155] In practical terms, these measures require enterprises 'to domestically store data related to their local business activities (domestic storage requirement), or require them to install data processing servers domestically (domestic facility installation requirement)'.[156]

As can be seen, DEPA, following the language used in the CPTPP, includes an extra layer (and complexity) to the GATS modeled exception. This additional layer specifies that the measure in question should not impose restrictions greater than necessary to achieve the legitimate public policy objective set by the concerned Party.

It should be noted that the RCEP presents a completely different path in this respect, 'perhaps influenced by the participation of China'.[157] China, with its newly implemented data protection and data security legal frameworks—the Personal Information Protection Law (PIPL) and the Data Security Law (DSL) adopted in 2021—'solidified and added to pre-existing data localization requirements', imposing obligations that can be considered as 'cumbersome' and a barrier to the free flow of data across borders'.[158] In this sense, 'China has established a comprehensive cross-border data flow regulatory regime, the core of which is "local storage, outbound assessment".[159]

This stance is evident in Article 12.14 of the RCEP. While no Party "shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that Party's territory" (Article 12.14.2), this rule is to be understood in the light of Article 12.14.3, which ensures a Party the possibility of adopting any measure "that it considers necessary to achieve a legitimate public policy objective, provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade" (a) or "any measure that it considers necessary for the protection of its essential security interests" (b). Article 12.14.3 (a) provision must be interpreted in line with its footnote, which states that "the Parties affirm that the necessity behind the implementation of such legitimate public policy shall be decided by the implementing Party". This implies that the mentioned rule is 'self-judging', i.e., 'anything can be deemed legitimate if a party says so'.[160] Furthermore, Article 12.14.3 (b) prevents other Parties from disputing the adoption or implementation of essential security interests protective measures. None of these limitations are present in the DEPA.

[155] Bacchus, 2021: 26.
[156] Abe, 2020: 2.
[157] Bacchus, 2021: 27.
[158] Dorwart, 2022: 2.
[159] Liu, 2020: 1.
[160] Leblond, 2020.

Another noteworthy issue arises when we compare the data localization rules found in the FTAs signed by Chile with Brazil and Uruguay with the text of the CPTPP and DEPA. It is possible to observe that the latter agreements introduce an additional step to the multi-tiered test ("does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective"). This addition holds significant relevance, as it opens the door to arguments in favor of voluntary self-regulatory approaches, as these would be less burdensome to achieve a legitimate public policy objective.

Table 1		
DEPA	***Article 4.4: Location of Computing Facilities*** The Parties affirm their level of commitments relating to location of computing facilities, in particular, but not exclusively: 1. The Parties recognise that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications. 2. No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory. 3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective.	
CHL Arg	***Article 11.7. Location of Computer Facilities*** 1. The Parties recognize the importance of not requiring a person of the other Party to use or locate computer facilities in the territory of that Party as a condition of doing business in that territory. 2. To this end, the Parties undertake to exchange best practices, experiences and existing regulatory frameworks with respect to server localization.	
CHL Bra	***Article 10.13. Location of Computer Facilities*** 1. The Parties recognize that each Party may have its own regulatory requirements relating to the use of computer facilities, including requirements that seek to ensure the security and confidentiality of communications. 2. A Party may not require a person of the other Party to use or locate computer facilities in the territory of that Party as a condition of doing business in that territory. 3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to pursue a legitimate public policy objective, provided that the measure is not applied in a manner that would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade.	
CHL Uru	***Article 8.11. Location of Computer Facilities*** 1. The Parties recognize that each Party may have its own regulatory requirements regarding the use of computer facilities, including requirements that seek to ensure the security and confidentiality of communications. 2. A Party may not require a person of the other Party to use or locate computer facilities in the territory of that Party as a condition for doing business in that territory. 3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the	

	measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade.	

It's important to point out that the commitments regarding the location of computer facilities in the Chile-Argentina FTA are comparatively less stringent when compared to the other mentioned agreements. In this FTA, signatories 'merely recognize the importance of not requiring a person of the other Party to use or locate the computer facilities in the territory of that Party, as a condition for conducting business in that territory and pledge to exchange good practices and current regulatory frameworks regarding servers' location'.[161]

e. Use of Encryption

Cryptography is increasingly used by businesses and for consumer goods and services to protect the confidentiality of data, such as financial or personal data, whether that data is in storage or in transit. In general terms, encryption refers to the use of security methods and privacy-enhancing technologies (PETs)[162] 'to encode data in transit or storage (or both) so that it can only be read by the authorized user'.[163]

These processes are used especially in ICT services contexts and data flows through different systems and organizations, transforming data in order 'to hide its information content, establish its authenticity, prevent its undetected modification, prevent its repudiation, and/or prevent its unauthorized use'.[164] Cryptography practices are 'the most fundamental technological basis for PETs', being increasingly viewed 'as promising approaches designed to prevent and mitigate the risk of privacy and confidentiality breaches and enable organisations to better manage data responsibly'.[165] Then, it is argued that encryption technologies and techniques play 'an important direct and indirect role in supporting digital trade',[166] making sure data is protected during 'transferring, the storage, and while it is displayed at destination'.[167]

Given the foregoing, the adoption in international agreements of measures that restrict or hinder the use of encryption technologies or techniques would have a negative impact on the privacy and protection of personal data of consumers and users. These restrictive policies would be motivated by the vision of certain governments and public bodies, who seek to 'maximize the reach of their investigatory powers'.[168] Consequently, some state actors consider that the use of strong encryption techniques could block access to user communications for public legitimate purposes, including law enforcement and domestic intelligence/security activities. Under this rationale, certain countries have moved towards implementing policies that come to 'weaken deployment of encryption in the private sector'.[169] These measures encompass actions such as the disclosure of encryption keys, granting requests by governments for

[161] Burri, 2022: 6.
[162] 'PETs typically can help reduce the risk of privacy and confidentiality breaches by minimising information disclosure', preventing 'any disclosure of data, unless strictly necessary to provide the envisaged functionality' (OECD, 2020: 23).
[163] UNCTAD, 2016: 52.
[164] OECD, 1997.
[165] OECD, 2020: 23.
[166] APEC Policy Support Unit, 2019: 88.
[167] UNDP Global Centre for Technology, Innovation, and Sustainable Development, 2021: 37.
[168] EPIC, n.d.
[169] EPIC, n.d.

decryption,[170] and the introduction of 'security flaws into [private sector] systems to be used as backdoors for law enforcement'.[171]

These types of policies, which aim to equip state actors with the means to access encrypted data through decryption support mandates, government-mandated encryption backdoors, and other bypass measures, can be viewed as directly undermining the security and privacy of personal data processing operations, negatively affecting safe and trustworthy data flows. Yet, these backdoors or disclosure requests can 'have explicit consequences in terms of an organisation's ability to achieve the certification requirements or adhere to the contractual conditions related to the transfer of data cross borders'.[172]

DEPA refers to encryption techniques in Article 3.4., on ICT products that use cryptography. This provision replicates the United States-Japan DTA Article 21 rule, which is similar to Annex 8-B, Section A.3 of the CPTPP Chapter on technical barriers to trade,[173] thereby prohibiting governments 'from requiring transfer or access to specific technologies as a condition for market access'.[174] In this sense, Article 3.4.3 of the DEPA states that 'no Party shall impose or maintain a technical regulation or conformity assessment procedure that requires a manufacturer or supplier of the product, as a condition of the manufacture, sale, distribution, import or use of the product, to: (a) transfer or provide access to a particular technology, production process or other information, for example, a private key [...]', which would also include other encryption backdoors.[175] Therefore, it could be interpreted that the language used by the DEPA in this regard, given that it follows the rule contained in Annex 8-B, Section A.3 of the CPTPP, would prevent a Party 'from requiring a supplier of cryptographic software to provide it with a backdoor or "golden key"'.[176]

However, as provided by the CPTPP and United States-Japan DTA Article 21, Article 3.4.5 of the DEPA states that this section 'shall not be construed to prevent a Party's law enforcement authorities from requiring service suppliers using encryption they control to provide, pursuant to that Party's legal procedures, unencrypted communications'.[177] It is worth mentioning that USMCA Article 12.C.2 and SADEA Article 7 'feature similar arrangements, though there is no analogous clause in the RCEP'.[178] This exception provides some latitude for interpretation or loopholes, giving governments a feasible alternative for obtaining encryption keys or encryption backdoors, so that 'it wouldn't do anything to prevent the government from seeking a court order against a software vendor requiring it to disclose the private key of a product that is lawfully marketed or supplied'.[179] Additionally, it is necessary to consider the provisions of Article 15.2 of the DEPA, 'Security Exceptions', which states, inter alia, that nothing in this agreement shall be constructed to 'preclude a Party from applying measures that it considers necessary for [...] the protection of its own essential security interests.'

Finally, it is important to highlight that the Chile-Uruguay FTA (Article 8.7.5), the Chile-Argentina FTA (Article 11.5.6) and the Chile-Brazil FTA (Article 10.8.6) encourage the use of encryption or other security

[170] APEC Policy Support Unit, 2019: 94.
[171] EPIC, n.d. In the case of APEC, some member economies are 'increasingly requiring encryption keys and data access', while others have implemented policies that require in fact 'breaking encryption' (APEC Policy Support Unit, 2019: 95).
[172] UNDP Global Centre for Technology, Innovation, and Sustainable Development, 2021: 37.
[173] Burri, 2021c: 91. Article 3.4 (2) of the DEPA, following the CPTPP, defines encryption as 'the conversion of data (plaintext) into a form that cannot be easily understood without subsequent re-conversion (ciphertext) through the use of a cryptographic algorithm'.
[174] Chang and Liu, 2022: 197.
[175] See Keitner and Clark, 2019: 6.
[176] Malcolm, 2015.
[177] Chang and Liu, 2022: 198.
[178] Ibid.
[179] Malcolm, 2015.

mechanisms for users' personal information, and their dissociation or anonymization, in case such data is provided to third parties.

VII. DEPA and International Regulation of Artificial Intelligence: Background

The Recommendation on Artificial Intelligence (AI), adopted by the Organisation for Economic Co-operation and Development (OECD) Council at Ministerial level on 22 May 2019 on the proposal of the Committee on Digital Economy Policy, defines "AI system" as 'a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy'.

AI technology-powered services 'rapidly diffuse across the global digital ecosystem'.[180] It is recognized that AI 'is already crossing borders, learning, making decisions, and operating cyber-physical systems'.[181] In view of the above, there has been in recent years a proliferation of different initiatives (at the domestic and international level) aimed at addressing some of the challenges that IA brings. When considering the challenges involved in the expansion of IA systems, it should be borne in mind that these technologies 'constitute complex socio-technical systems involving humans, machines, algorithms, and data, and their deployment raises legal questions across a wide range of domains, including but not limited to data protection and privacy law, antidiscrimination law, intellectual property law, and tort law'.[182]

In general terms, efforts to build a set of standards that govern the use and adoption of AI have concentrated on two categories of policies: the development of principle-based ethical recommendations or high-level goals guidelines, with a multidisciplinary approach; and, the introduction of legal rules and provisions applicable to these technologies, including a special set of obligations to be followed by entities that create, deploy, and use these technologies, along with ensuring the adequate protection of the fundamental rights of individuals who may be affected by these systems.[183]

From an international law perspective, we are witnessing the gradual emergence of a flexible "soft law" approach to governing AI. Within this scenario, international organizations, technical standardization organizations, private business and civil society have adopted an active role in the discussion of these ground rules, focused on identifying appropriate regulatory approaches and defining initial non-binding frameworks, bearing in mind the challenges arising from rapid technological change.[184]

Although these difficulties are not new in the field of regulatory law,[185] it is particularly acute in international law. This hindrance, known as the "pacing problem", implies that when addressing technology regulation, it is difficult to foresee or anticipate the effects and impact that a regulatory proposal will have on the matter covered by its rules. In this sense, it is possible to assert that oversight and governance do not keep pace with technological and scientific change.[186] Regarding this pacing problem, two factors should be highlighted. First, there is the issue of regulatory obsolescence, which occurs when technological

[180] Irion, 2021: 3.
[181] Chander, 2021: 116.
[182] Peng et al., 2021: 3.
[183] Contreras and Trigo, 2021: 457.
[184] 'In some areas, certain forerunner countries, notably, the US, China, and the European Union (EU) have attempted to govern AI and other disruptive technologies. [...] In others, governments have begun to reach out to their counterparts to update the existing framework—be it loosely organized trans-governmental networks or treaty-based mechanisms. Further, various industry stakeholders have also engaged one another or even teamed up with regulatory agencies to coordinate their activities' (Liu and Ching-Fu, 2020: 305).
[185] Hagemann et al., 2018: 42 ff.
[186] Askland, 2011: xiii.

evolution speeds up exponentially[187] (i.e., rules designed to govern a specific technology prove useless once the technology changes or falls into disuse). Secondly, the anticipation problem, that results from the "static" nature of regulation, and bureaucratic deficiencies to face these new challenges.[188]

Although the rules contained in free trade agreements could 'serve as a laboratory for new trade rules',[189] including AI regulation, certain challenges must be borne in mind, not only in terms of the proportionality and effectiveness of these prospective rules, but also in relation to the need to avoid creating a behind-the-border barrier to digital services trade.[190]

a. Article 8.2. of DEPA: Analysis

DEPA incorporates a special module (8) on emerging trends and technologies. Article 8.2 addresses in particular certain aspects related to the use and adoption of AI technologies.

Box 6

Article 8.2: Artificial Intelligence

1. The Parties recognise that the use and adoption of Artificial Intelligence (AI) technologies have grown increasingly widespread in the digital economy.

2. The Parties recognise the economic and social importance of developing ethical and governance frameworks for the trusted, safe and responsible use of AI technologies. In view of the cross-border nature of the digital economy, the Parties further acknowledge the benefits of developing mutual understanding and ultimately ensuring that such frameworks are internationally aligned, in order to facilitate, as far as possible, the adoption and use of AI technologies across the Parties' respective jurisdictions.

3. To this end, the Parties shall endeavour to promote the adoption of ethical and governance frameworks that support the trusted, safe and responsible use of AI technologies (AI Governance Frameworks).

4. In adopting AI Governance Frameworks, the Parties shall endeavour to take into consideration internationally recognised principles or guidelines, including explainability, transparency, fairness and human-centred values.

Through a soft language approach, the Parties acknowledge the increasing prevalence of AI in the digital economy and recognize the importance of developing ethical and governance frameworks to ensure the trusted, safe, and responsible use of AI technologies. They also highlight the benefits of aligning these frameworks internationally to facilitate their adoption across different jurisdictions. Furthermore, they commit to promoting the adoption of such ethical and governance frameworks (AI Governance Frameworks) that support the responsible use of AI technologies. When adopting these frameworks, Parties shall strive to consider internationally recognized principles and guidelines, including factors like explainability, transparency, fairness, and human-centric values.

[187] Marchant, 2011: 20-23.
[188] Hageman et al., 2018: 63-65.
[189] Wunsch-Vincent and Hold, 2012: 193.
[190] Chander, 2021: 127.

From the above-mentioned text, it can be concluded that, in substance, the Parties limit their commitment in these matters to endeavour to promote the adoption of AI Governance Frameworks, i.e., 'ethical and governance frameworks that support the trusted, safe and responsible use of AI technologies'. The language used is open-ended and indeterminate, which does not make it possible to specify the scope of these non-binding commitments, nor does it provide clear guidelines on the framework that the Parties should develop. For example, the difference between ethical criteria and governance criteria is not clarified, e.g., whether this distinction relates to their (lack of) binding effect. Article 8.2 approach is highly flexible, merely enunciating four basic principles to keep in mind in the development of AI Governance Frameworks (explainability, transparency, fairness and human-centred values)[191] without elaborating their content. It also emphasizes the importance of aligning these frameworks with international standards. These elements—the list of basic principles and the need to take into consideration internationally recognised guidelines—constitute the only criteria that would substantially guide the application of this provision. Nevertheless, this pragmatic approach 'disincentivises unilateral approaches inconsistent with international best practices'.[192]

It is possible to argue that this is an area 'where the agreement has only established a roadmap for the future', being a 'starting point for multilateral rulemaking around the digital economy'.[193] In some areas, including AI, DEPA only puts in place an 'undertaking to collaborate on the development of new rules, new policy approaches or improved 'interoperability' (either technical or regulatory) to help systems to work seamlessly across the three countries'.[194] Thus, in these matters, an approach limited only to cooperation was adopted.

Has this soft-approach influenced other next-generation free trade agreements? The SADEA, signed on August 6, 2020, is Singapore's second Digital Economy Agreement after the DEPA (given that DEPA was signed in June 2020, negotiations of both DEPA and SADEA would have run in parallel). Article 31 SADEA addresses AI issues following a similar logic to that contained in Article 8.2 DEPA.[195] However, both provisions differ in some elements. For instance, the SADEA does not refer to a list of basic AI principles. The incorporation of principles in AI modules, although non-binding, may be relevant to the process of discussing and shaping the first binding regulatory instruments for AI, based on their challenges and risks, 'aligning AI design and use with human rights, democracy, and the rule of law'.[196] It is also noteworthy that in 2019 some AI ethical principles were already agreed, 'such as those in the OECD Recommendation on AI, and the G20 non-binding principles on AI'.[197]

Another notable aspect to consider is the inclusion of source code clauses within free trade agreements, that could restrict, to some extent, AI governance and regulation.[198] In this regard, it can be observed a proliferation of a source code disciplines in regional trade agreements (introduced 'for the first time by the US in the Trans-Pacific Partnership negotiations'),[199] including the CPTPP,[200] the USMCA, and the

[191] Jones et al., 2021: 38.
[192] Mishra, 2022: 8.
[193] García and Rebolledo, 2020.
[194] Honey, 2020.
[195] See Mishra, 2022.
[196] Leslie et al., 2021: 24.
[197] Leslie et al., 2021: 5. However, Article 8.2 of the DEPA raises questions due to its omission of key aspects that are crucial in the context of AI. These include the need to ensure respect for fundamental rights, the necessity of AI human oversight, and the concept of accountability.
[198] See Irion, 2021
[199] Mishra, 2022: 9.
[200] Article 14.17: Source Code. 'Pursuant to Article 14.17, a CPTPP Member may not require the transfer of, or access to, source code of software owned by a person of another Party as a condition for the import, distribution, sale or use

SADEA.[201] For instance, in the case of the USMCA, Article 19.16 (Source Code) establishes a limitation on the ability of governments to require the transfer of, or access to, an algorithm expressed in a source code of software owned by a person of another Party.[202] It's worth highlighting that this provision explicitly covers algorithms, which, according to Article 19.1, are 'a defined sequence of steps, taken to solve a problem or obtain a result'. The SADEA provides in Article 28.4 a similar discipline if both Parties undertake equivalent obligations under an international agreement or an amendment to any existing international agreement that comes into force after SADEA.

This type of provision has a direct effect on the governance of AI algorithms, as 'computer and machine learning algorithms when they are expressed in source code fall inside the scope of such a trade law clause', which 'may already turn out too restrictive for domestic digital policies that need to build on interoperability, accountability, and verifiability' of new algorithm-based technologies.[203] Among other important aspects, access to software source code may be indispensable in order 'to meet regulatory and judicial needs in order to ensure that digital technologies are in conformity with individuals' human rights and societal values'.[204] On the other hand, exceptions allowing regulatory bodies and judicial authorities to access source code and algorithms for a specific investigation, inspection, examination, enforcement action, or judicial proceeding (such as those contained in the USMCA) 'can be vague and unclear regarding what type of procedures and investigations would qualify for such access to be granted. The focus on disclosure of relevant source codes to public authorities and regulatory bodies also means that, in important cases, it may not be possible to share the source code with individuals who might be affected by automated decision-making'.[205]

While DEPA covers 'a wider range of issues than those typically found in most PTAs [...] there are a few issues that this agreement does not touch upon, even though previous agreements have addressed them in some way'.[206] In this sense, the absence of a provision on source code in the DEPA is rather remarkable, considering that 'all three parties to the agreement have signed other PTAs that prohibit the imposition of trade restrictive measures related to the disclosure, transfer of and access to source code'.[207] This could be considered a 'belated recognition of problems that these rules pose for competition authorities, anti-discrimination law, cybersecurity and other areas of public policies'.[208] Additionally, it should not be overlooked that FTAs' commitments aimed at protecting software source code against government access and transfer can render 'a double-edged sword that can be used to contest a country's measure in pursuit of algorithmic transparency, fairness and accountability'.[209]

In this specific regard, DEPA is similar to RCEP, which 'does not contain any provision regarding source code'.[210] It must however be borne in mind that art. 12.16.1 RCEP states that 'Parties have agreed to discuss

---

of such software, or of products containing such software, in its territory. The prohibition applies only to mass market software or products containing such software' (Burri, 2021b: 35).

[201] Such provisions could 'be interpreted as a reaction to China's demands to access to source code from software producers selling in its market' (Burri, 2021c: 86).

[202] '[T]o the regulatory body for a specific investigation, inspection, examination, enforcement action, or judicial proceeding, subject to safeguards against unauthorized disclosure'. Footnote 6 adds '[t]his disclosure shall not be construed to negatively affect the software source code's status as a trade secret, if such status is claimed by the trade secret owner'.

[203] Irion, 2022: 1566.

[204] Irion, 2022: 1561.

[205] Jones et al., 2021: 34.

[206] Soprana, 2021: 163.

[207] Ibid.

[208] Kelsey, 2020.

[209] Irion, 2022 : 1563.

[210] Leblond, 2020.

source code as one of the emerging issues that should be considered in future dialogues on e-commerce'.[211] In summary, DEPA has notable implications for emerging AI regulation because of what it lacks—specifically, improved protections for source code. Consequently, it can be inferred that DEPA, in contrast to other new trade agreements, refrains from creating barriers for participating parties to implement domestic measures aimed at achieving algorithmic transparency, fairness, and accountability through access to source codes or their algorithms.

VIII. Can the DEPA be Considered a Pathfinder for the Future Regulation of Cross-Border Data Flows, and What Effect Might This Have on the Regulatory Margin of Discretion that Countries Currently Have?

DEPA 'builds upon the digital trade or e-commerce chapters of existing free trade agreements'.[212] The Joint Ministerial Statement on the substantial conclusion of Digital Economy Partnership Agreement negotiations[213] highlights DEPA's forward-looking character, seen as a comprehensive pathfinder built on existing trade agreement commitments. Accordingly, some DEPA provisions 'pick up and refine existing rules',[214] building heavily on the CPTPP.[215] In this regard, it is argued that CPTPP model rapidly emerged as 'the standard approach in "modernized" trade deals featuring e-commerce or digital trade rules', including both large and small trade agreements.[216]

The 'most important textual source is the CPTPP, to which all three DEPA members are party',[217] replicating or reiterating commitments already made by the parties.[218] So, for instance, '[i]n several respects, the DEPA builds on the innovations on digital trade in chapter 14 of the CPTPP',[219] on electronic commerce.

It is difficult to claim that the DEPA could be considered a trailblazer for future cross-border data flow regulations. However, two issues deserve our attention: the first is that because of its modular approach and uncompromising wording, it is an agreement that arouses growing interest. The second is that even if no concrete commitments are made regarding data flows, this does not mean that DEPA declarations cannot have any legal relevance. On the contrary, different legal effects could derive from these declarations, especially as more countries join the agreement.

In this context, it is important to consider that this treaty is inserted in a broader context, intertwined with other trade agreements in which DEPA Parties are engaged. Statements made in the DEPA could be considered in an international dispute settlement, even when the dispute does not emanate directly from DEPA's specific provisions. Moreover, these statements could play a significant role in resolving disputes arising from breaches of other commitments made within DEPA that are not excluded from Module 14

---

[211] Jones et al., 2021: 37.

[212] Government of Canada, 25 August 2022, *Background: Canada's possible accession to the Digital Economy Partnership Agreement*. Available at: https://www.international.gc.ca/trade-commerce/consultations/depa-apen/background-information.aspx?lang=eng

[213] http://www.sice.oas.org/TPD/DEPA/Negotiations/DEPA_Jnt_Stmt_conclusion_e.pdf

[214] Asia Trade Centre, 2020.

[215] Soprana, 2021: 168.
In this sense, the original plan to sign a final agreement just six months later the Joint Ministerial Statement issued in May 2019 'inevitably required drawing heavily on existing agreements' (Kelsey, 2020).

[216] Geist, 2018.

[217] Fay and Ciuriak, 2022a: 3.

[218] Thus, with respect to CPTPP signatory countries, it is held that DEPA membership means 'essentially agree to provisions already in force' (Fay and Ciuriak, 2022b).

[219] Bacchus, 2021: 18

(dispute settlement), when the crux of the matter pertains not to the correct interpretation or application of Article 4.3. Moreover, it is worth noting that while Module 14 does not extend to Article 4.3 (Cross-Border Transfer of Information by Electronic Means), it is indeed applicable to Article 4.2 (Protection of Personal Information), which states, in paragraph 10, that "the Parties shall endeavour to mutually recognise the other Parties' data protection trustmarks as a valid mechanism to facilitate cross-border information transfers while protecting personal information." Additionally, the fact that under Annex I of the DEPA, Article 4.3 does not create any rights or obligations between the Parties should not necessarily be interpreted to mean that such provision does not create rights and obligations at all, or that it cannot be considered in other agreements.

It should not be overlooked that the commitments undertaken in the DEPA could have an impact on investor-state dispute settlement, for instance, to interpret what constitutes the international minimum standard that the host country should observe concerning foreign investors, or to determine in which case a measure taken by a state could constitute indirect expropriation. In this sense, the practice of states in concluding treaties 'is capable of strengthening the alleged rules of customary international law'.[220] Investment disputes generally involve a claim of liability of the host state for some form of indirect expropriation carried out without compensation or in violation of the principle of fair and equitable treatment. [221] For instance, a change in regulations pertaining to privacy or personal data transfers can significantly escalate a company's operational expenses within a specific country. Such regulatory shifts may be perceived as a form of indirect expropriation by investors who initiated business activities in that country under less stringent data protection regulations.

This is an area where judges often employ various interpretative elements to adjudicate disputes. Consequently, many of the decisions rendered in this context have generated concerns, primarily due to perceptions of overreach or excessive creativity in interpreting rules of foreign investment law, such as those relating to indirect expropriation or fair and equitable treatment in favor of foreign investors, at the expense of the legitimate sovereignty of host states, including the regulatory or "police" powers of states.[222] Furthermore, this domain has witnessed robust growth in recent years, with particularly pronounced effects on developing countries. The rapid expansion can be attributed to both the substantial costs involved in investment dispute resolution and its significant political ramifications.

[220] Subedi, 2008: 85. It should be noted that 'Module 1 of DEPA stipulates that the parties' existing agreements still co-exist. Ambiguity arises as DEPA is silent on the status of future agreements. While any inconsistency with another agreement is subject to consultation, it is currently unclear whether it would go to a dispute under DEPA or the other treaty' (Kelsey, 2020). In this sense, the issue of DEPA's relationship with the CPTPP resurfaces. The original negotiating parties will have assumed that for enforcement they would rely on the CPTPP dispute mechanism. With non-CPTPP parties, if the data provisions are made part of DEPA they could be covered under its dispute mechanism, although it is unclear what remedies might realistically apply.
[221] Subedi, 2008: 119.
[222] Subedi, 2008: 143.

IX. Conclusions

Digital transformation stands as a pivotal catalyst for growth and innovation in today's global economy. The rapid expansion of the digital landscape, coupled with innovative business models, has accentuated the compelling necessity to establish suitable trade regulations and governance mechanisms that effectively address digital trade's main challenges.

Undoubtedly, the collection, processing, and sharing of personal data have assumed a central role in the modern data-centric digital economy. It is increasingly evident that data flows constitute the bedrock upon which cross-border digital trade is built, thus underscoring the growing consensus regarding the need for enhancing global digital data governance.

Despite this matter's increasing importance, it has yet to be possible to achieve an international consensus to comprehensively tackle the diverse aspects of digital trade at the multilateral level. As a result, it has become more common to encounter digital trade provisions incorporated into new free trade agreements, resulting in what is often described as a 'spaghetti bowl' of regulations in the digital trade sphere. This has given rise to distinct visions or models, prominently exemplified by the proliferation of the 'US-led digital trade template,' which prioritizes the free flow of data.

In this scenario, the question arises whether the DEPA, one of the pioneering comprehensive international agreement on digital trade, could be considered a pathfinder in shaping global rules for cross-border data flows. DEPA is frequently touted as an innovative free trade agreement, especially in terms of its adaptable design and modular approach. Consequently, new parties can determine the extent of their commitment, without being bound to fully embrace the entirety of the agreement.

As demonstrated in this paper, when examining the rules concerning data flows governance, the DEPA closely aligns with the approach championed by the United States during the TPP negotiations. It's important to note that even though the United States is not a participant in the CPTPP, its provisions draw heavily from the TPP, where the US played a significant role in shaping the negotiation process. The similarity might be attributed to the relatively brief negotiation period for DEPA, which 'inevitably required drawing heavily on existing agreements'.[223] Consequently, especially regarding cross-border data flows, DEPA does not pave a new direction but rather the continuation of the one traced by the United States. This circumstance has a decisive impact on the added value offered by this digital trade agreement.

DEPA rules governing cross-border data flows (Article 4.3) take verbatim CPTPP cross-border transfer of information provision, also affirming parties' previous levels of commitment contained in other agreements. As highlighted in the report, this situation can pose significant challenges. Questions arise about which prior agreements would set parties' "level of commitments relating to cross-border transfer", mainly when they may exist inconsistent or contradictory rules. The complexity is further heightened when considering countries that are not part of the CPTPP. These factors could hurt the likelihood of new DEPA parties embracing all its modules. Despite DEPA's personal information protection provisions being more detailed than the CPTPP text, they 'fail to set minimum standards'.[224] Furthermore, DEPA strongly promotes interoperability through the adoption and mutual recognition of voluntary self-regulatory approaches, which could be considered in some way equivalent to the implementation of comprehensive or sectoral privacy/data protection laws. On the other hand, from the detailed review of Article 4.2, on personal information protection, it is possible to note that DEPA, taking as its basis Article 14.8 of CPTPP, introduces some new elements that seem to reveal an intention not only to maintain the commitments reached in the CPTPP but also to deepen data transfer obligations.

[223] Kelsey, 2020.
[224] Ibid.

As observed in the case of Chile, the shift towards interoperability entails aligning more closely with the US model and moving away from the approach taken in certain bilateral FTAs concluded before the commencement of DEPA's negotiation process. The course followed by Chile in South America aims at achieving regulatory convergence in the domain of data privacy/data protection. This convergence is underpinned by laws or administrative regulations geared towards safeguarding the personal information of users engaged in electronic commerce. The ultimate goal, as demonstrated in the Chile-Argentina FTA, is to ensure that individuals receive a level of protection that is at least as strong as the legal and administrative provisions in place in the exporting country, preserving their rights.

In the global context where consensus on data governance rules remains elusive due to divergent and often conflicting approaches, the fact that one of the first comprehensive international agreement on digital trade has adopted the US model does not seem innocuous. Specifically, with regard to cross-border data flows, DEPA does not forge a new path but rather follows the trajectory set by the United States. This circumstance has a decisive impact on the added value offered by this digital trade agreement. If we consider that DEPA has been specially conceived and designed as a pathfinder to 'influence and contribute to multilateral trade negotiations on digital trade',[225] it is not difficult to imagine that a broad accession or replication of its terms and provisions could end up producing a *de facto* harmonization under the US data governance model.

[225] Soprana, 2021: 168.

References

Aaronson, S. (2021). *Agreement Biden Should Sign Up For Now.* Barron's, 1 March 2021. Available at: https://www.barrons.com/articles/the-one-trade-agreement-biden-should-sign-up-for-now-51614607309

Aaronson, S. (2019). "Data is Different: Why the World Needs a New Approach to Governing Cross-border Data Flows". Working Papers 2018-10, The George Washington University, Institute for International Economic Policy. Available at: https://www2.gwu.edu/~iiep/assets/docs/papers/2018WP/AaronsonIIEP2018-10.pdf

Aaronson, S. (2018). *Data Minefield: How AI is Prodding Governments to Rethink Trade in Data*. Centre for International Governance Innovation, 3 April 2018. Available at: https://www.cigionline.org/articles/data-minefield-how-ai-prodding-governments-rethink-trade-data/

Aaronson, S., Kimura, F., Lee-Makiyama, H. and Stephenson, S. (2021). "Actions to make 'data free flow with trust' operational in practice". Policy Brief, G20 Insights, 30 September. Available at: https://www.g20-insights.org/policy_briefs/actions-to-make-data-free-flow-with-trust-operational-in-practice/

Aaronson, S. and Leblond, P. (2018). "Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO". *Journal of International Economic Law*, 21(2), 245-272.

Abe, Y. (2020). "Data Localization Measures and International Economic Law: How Do WTO and TPP/CPTPP Disciplines Apply to These Measures?". *Public Policy Review*, 2020, vol. 16, issue 5, 1-29.

Agrawal, B. and Mishra, N. (2022). "Addressing the Global Data Divide through Digital Trade Law". *14(2) Trade, Law & Development* (2022). Available at SSRN: https://ssrn.com/abstract=4276764 or http://dx.doi.org/10.2139/ssrn.4276764

Asia-Pacific Economic Cooperation (APEC) Policy Support Unit (2019). *Fostering an Enabling Policy and Regulatory Environment in APEC for Data-Utilizing Businesses.* Available at: https://www.apec.org/publications/2019/07/fostering-an-enabling-policy-and-regulatory-environment-in-apec-for-data-utilizing-businesses

Asia Trade Centre (2021). *China applies to join DEPA.* 4 November 2021. Available at: http://asiantradecentre.org/talkingtrade/china-applies-to-join-depa

Asia Trade Centre (2020). *Unpacking The Digital Economy Partnership Agreement (DEPA)*. 28 January 2020. Available at: http://asiantradecentre.org/talkingtrade/unpacking-the-digital-economy-partnership-agreement-depa

Askland, A. (2011). "Introduction: Why law and ethics need to keep pace with emerging technologies". In G. E. Marchant *et al.* (eds.), *The growing gap between emerging technologies and legal-ethical oversight. The pacing problem* (New York: Springer).

Association of Southeast Asian Nations (ASEAN) (2017). *Framework On Digital Data Governance.* Available at: https://asean.org/wp-content/uploads/2012/05/6B-ASEAN-Framework-on-Digital-Data-Governance_Endorsedv1.pdf

Bacchus, J. (2021). *The Digital Decide. How to Agree on WTO Rules for Digital Trade*. Centre for International Governance Innovation. Available at: https://www.cigionline.org/publications/the-digital-decide-how-to-agree-on-wto-rules-for-digital-trade/

Bennett, C. (2020). *The Council of Europe's Modernized Convention on Personal Data Protection: Why Canada Should Consider Accession*. Centre for International Governance Innovation - CIGI Papers No. 246 — November 2020. Available at: https://www.cigionline.org/static/documents/documents/no246_0.pdf

Blume, J. (2018). "Reading the Trade Tea Leaves- A Comparative Analysis of Potential United States WTO-GATS Claims Against Privacy, Localization, and Cybersecurity Laws". *Georgetown Journal of International Law*, Volume 49, Issue 2 (Winter 2018), 801.

Burri, M. (2022). "Creating Data Flows Rules through Preferential Trade Agreements". Forthcoming in: Anupam Chander and Haochen Sun (eds), *Data Sovereignty along the Digital Silk Road* (Oxford: Oxford University Press, 2022), Available at SSRN: https://ssrn.com/abstract=3910408 or http://dx.doi.org/10.2139/ssrn.3910408

Burri, M. (2021a). "Data Flows versus Data Protection: Mapping Existing Reconciliation Models in Global Trade Law". In K. Mathis and A. Tor (eds), *The Law and Economics of Regulation* (Cham: Springer).

Burri, M. (2021b). "Data Flows and Global Trade Law". In M. Burri (Ed.), *Big Data and Global Trade Law* (pp. 11-41). Cambridge: Cambridge University Press.

Burri, M. (2021c). "Towards a New Treaty on Digital Trade". *Journal of World Trade* 55(1), 77–100.

Burri, M. (2021d). "Approaches to Digital Trade and Data Flow Regulation across Jurisdictions: Implications for the Future EU–ASEAN Agreement". *Legal Issues of Economic Integration* 49 (2022), 149–168, Available at SSRN: https://ssrn.com/abstract=3804975

Burri, M (2021e). "Interfacing Privacy and Trade". 53 *Case W. Res. J. Int'l L.* 35. Available at: https://scholarlycommons.law.case.edu/jil/vol53/iss1/5

Burri, M. (2017). "The Regulation of Data Flows Through Trade Agreements". *Law and Policy in International Business* 48(1): 407-448

Business Wire (2020). *IDC Reveals 2021 Worldwide Digital Transformation Predictions; 65% of Global GDP Digitalized by 2022, Driving Over $6.8 Trillion of Direct DX Investments from 2020 to 2023. 29 October 2020*. Available at: https://www.businesswire.com/news/home/20201029005028/en/IDC-Reveals-2021-Worldwide-Digital-Transformation-Predictions-65-of-Global-GDP-Digitalized-by-2022-Driving-Over-6.8-Trillion-of-Direct-DX-Investments-from-2020-to-2023

Chander, A. (2021). "Artificial Intelligence and Trade". In Mira Burri (ed), *Big Data and Global Trade Law* (Cambridge: Cambridge University Press), 115-127.

Chang, L. Y. C. and Liu, H. W. (2022). "Ensuring Cybersecurity for Digital Services Trade". In Jong Woo Kang, Matthias Helble, Rolando Avendano, Pramila Crivelli, & Mara Claire Tayag (eds). *Unlocking the Potential of Digital Services Trade in Asia and the Pacific*. Asian Development Bank.

Chen, Y. (2020). “Improving market performance in the digital economy”. *China Economic Review*, Volume 62.

Chin, Y. C. and Zhao, J. (2022). ‘Governing Cross-Border Data Flows: International Trade Agreements and Their Limits’. *Laws* 11: 63. https://doi.org/10.3390/laws11040063

Congressional Research Services (2021). *Digital Trade and U.S. Trade Policy*. Updated December 9, 2021. Available at: https://crsreports.congress.gov/product/pdf/R/R44565

Congressional Research Services (2020). *Data Flows, Online Privacy and Trade Policy*. Available at: https://crsreports.congress.gov/

Contreras, P. and Trigo, P. (2021). “La gobernanza de la inteligencia artificial. Esbozo de un mapa entre hard law y soft law internacional”. In Michelle Azuaje and Pablo Contreras (eds), *Inteligencia artificial y Derecho: Desafíos y perspectivas* (Valencia: Tirant Lo Blanch), 457-480.

Creemers, R. (2020). *China’s Approach to Cyber Sovereignty* (Berlin: Konrad-Adenauer-Stiftung e. V.). Available at: https://www.kas.de/documents/252038/7995358/China’s+Approach+to+Cyber+Sovereignty.pdf/2c6916a6-164c-fb0c-4e29-f933f472ac3f?version=1.0&t=1606143361537

de Hert, P. and Papakonstantinou, V. (2015). “The data protection regime in China. In-depth Analysis”. Brussels Privacy Hub Working Paper Vol. 1, N° 4, November 2015. Available at: https://brusselsprivacyhub.eu/BPH-Working-Paper-VOL1-N4.pdf

Dorwart, H. (2022). *Demystifying Data Localization in China: a Practical Guide*. Future of Privacy Forum. Available at: https://fpf.org/wp-content/uploads/2022/02/Demystifying-Data-Localization-Report.pdf

Electronic Privacy Information Center (EPIC) (n.d.). *Encryption. Cybersecurity Issues*. Available at: https://epic.org/issues/cybersecurity/encryption/

Erie, M. S. and Streinz, T. (2021). “The Beijing Effect: China’s Digital Silk Road as Transnational Data Governance”. 54 *N.Y.U. J. Int’l L. & Pol*. 1

European Agency for Fundamental Rights (FRA) (2018). *Handbook on European data protection law - 2018 edition* (Luxemburg: Publications Office of the European Union).

European Commission (n.d.). *Adequacy decisions. How the EU determines if a non-EU country has an adequate level of data protection*. Available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

European Parliament (2020). *Legal Analysis of International Trade Law and Digital Trade. Policy Department for External Relations*. Available at: https://www.europarl.europa.eu/thinktank/en/document/EXPO_BRI(2020)603517

Fay, R. and Ciuriak, D. (2022a). “The Digital Economic Partnership Agreement: Should Canada Join?”, Policy Brief 171 - January 2022, Centre for International Governance Innovation. Available at: https://www.cigionline.org/static/documents/PB_no.171.pdf

Fay, R. and Ciuriak, D. (2022b). *Digital Economy Partnership Agreement Is a Big Step Forward: Canada Should Join*. Centre for International Governance Innovation (CIGI), 14 April 2022. Available at: https://www.cigionline.org/articles/digital-economy-partnership-agreement-is-a-big-step-forward-canada-should-join/

Feifei, F. (2021). *China files formal application to join DEPA*. China Daily, 1 November 2021. Available at: https://global.chinadaily.com.cn/a/202111/01/WS617f640ba310cdd39bc7291e.html

Foreign Trade Information System of the OAS (SICE) (n.d.). *Digital Economy Partnership Agreement (DEPA), Background and Negotiations*. Available at: http://www.sice.oas.org/TPD/DEPA/DEPA_e.ASP

Foreign Trade Information System of the OAS (SICE) (n.d.). Comprehensive and Progressive Agreement for Trans Pacific Partnership Agreement (CPTPP) - Australia, Brunei Darussalam, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, and Vietnam, *Background and Negotiations*. Available at: http://www.sice.oas.org/tpd/tpp/tpp_e.asp

Gao, H. (2018). "Regulation of Digital Trade in US Free Trade Agreements: From Trade Regulation to Digital Regulation". 45, *Legal Issues of Economic Integration*, Issue 1, 47-70.

Garcia, P. M. and Rebolledo, A. (2020). *The Digital Economy Partnership Agreement, a milestone in trade negotiations*. Inter-American Development Bank blogs (Blogs iadb), 15 September 2020. Available at: https://blogs.iadb.org/integration-trade/en/the-digital-economy-partnership-agreement-a-milestone-in-trade-negotiations/

Gascón Marcén, A. (2021). "The Regulation of personal data flows between the European Union and the Asia-Pacific Region". *Australian and New Zealand Journal of European Studies*, Vol 13 (2): 30-41.

Geist, M. (2018) *Data rules in modern trade agreements. Toward Reconciling an Open Internet with Privacy and Security Safeguards*. Centre for International Governance Innovation. Available at: https://www.cigionline.org/articles/data-rules-modern-trade-agreements-toward-reconciling-open-internet-privacy-and-security/

Greenleaf, G. (2022). 'Global CBPRs: A Recipe for Failure?' 177 *Privacy Laws & Business International Report* 11-13, Available at SSRN: https://ssrn.com/abstract=4180516 or http://dx.doi.org/10.2139/ssrn.4180516

Greenleaf, G. (2020). "Will Asia-Pacific Trade Agreements Collide with EU Adequacy and Asian Laws?". 167 *Privacy Laws & Business International Report* 18-21, Available at SSRN: https://ssrn.com/abstract=3753215 or http://dx.doi.org/10.2139/ssrn.3753215

Greenleaf, G. (2019) 'It's Nearly 2020, so What Fate Awaits the 1980 OECD Privacy Guidelines? (A Background Paper for the 2019 OECD Privacy Guidelines Review)'. 159 *Privacy Laws & Business International Report*, 18-21, UNSW Law Research Paper No. 19-42, Available at SSRN: https://ssrn.com/abstract=3405156

Greenleaf, G. (2013). 'Modernising' data protection Convention 108: A safe basis for a global privacy treaty? *Computer Law & Security Review*, Vol. 29, Issue 4, 430-436.

Greenleaf, G. and Waters, N. (2012). 'Obama's Privacy Framework: An Offer to be Left on the Table?'. *Privacy Laws & Business International Report*, No. 119, 6-9, October 2012 , UNSW Law Research Paper No. 2012-56. Available at SSRN: https://ssrn.com/abstract=2187234

Greenleaf, G. (2009). "Five Years of the Apec Privacy Framework: Failure or Promise?". *Computer Law & Security Report*, Vol. 25, 28-43. Available at SSRN: https://ssrn.com/abstract=2022907

Hagemann, R. (2018). "Soft law for hard problems: The governance of emerging technologies in an uncertain future". *Colo. Tech. L.J.* (Vol. 17, Nº 1), 37-129.

Heda, S. (2016). *Trans Pacific Partnership and Digital 2 Dozen: Implications for Data Protection and Digital Privacy*. Centre for Internet & Society (CIS). 12 July 2016. Available at: https://cis-india.org/internet-governance/blog/tpp-and-d2-implications-for-data-protection-and-digital-privacy.

Henckels, C. (2016). "Protecting Regulatory Autonomy through Greater Precision in Investment Treaties: The TPP, CETA, and TTIP". *Journal of International Economic Law*, Volume 19, Issue 1, March 2016, 27–50.

Honey, S. (2021). *Enabling trust, trade flows, and innovation: the DEPA at work*. Hinrich Foundation. Available at: https://www.wita.org/wp-content/uploads/2021/07/The-DEPA-at-work-Hinrich-Foundation-white-paper-Stephanie-Honey-July-2021-RV.pdf

Honey, S. (2020). *Digging DEPA: the Digital Economy Partnership Agreement*. Trade Working Blog, 16 June 2020. Available at: https://tradeworks.org.nz/digging-depa-the-digital-economy-partnership-agreement/

Huld, A. (2021). *Can China Join the Digital Economy Partnership Agreement?*. China Briefing, 19 November 2021. Available at: https://www.china-briefing.com/news/can-china-join-the-digital-economy-partnership-agreement/

Hufbauer, G. C. and Hogan, M. (2021). "Digital agreements: What's covered, what's possible". Policy Briefs PB21-22, Peterson Institute for International Economics. Available at: https://www.piie.com/sites/default/files/documents/pb21-22.pdf

Inha Jeonse University Gazette (2022). *The Digital Economy Partnership Agreement, a Milestone in Trade Negotiations*. Available at: http://www.inhapress.com/news/articleView.html?idxno=10364

Irion, K. (2022). 'Algorithms Off-limits?: If digital trade law restricts access to source code of software then accountability will suffer'. 2022 *ACM Conference on Fairness, Accountability, and Transparency (FAccT '22)*, June 21–24, 2022, Seoul, Republic of Korea. ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3531146.3533212

Irion, K. (2021). *AI Regulation in the European Union and Trade Law: How Can Accountability of AI and a High Level of Consumer Protection Prevail over a Trade Discipline on Source Code?* (Berlin: Verbraucherzentrale Bundesverband e.V.).

Irion, K., Yakovleva, S. and Bartl, M. (2016). *Trade and Privacy: Complicated Bedfellows? How to achieve data protection-proof free trade agreements* (independent study commissioned by BEUC

et al.). Amsterdam, Institute for Information Law (IViR). Available at: https://www.ivir.nl/publicaties/download/trade_and_privacy.pdf

Ismail, Y. (2021). *E-commerce Joint Statement Initiative Negotiations Among World Trade Organization Members: State of play and the impacts of COVID-19*. International Institute for Sustainable Development (IISD). Available at: https://policycommons.net/artifacts/1526545/e-commerce-joint-statement-initiative-negotiations-among-world-trade-organization-members/2214778/

Jones, E., Garrido Alves, D. B, Kira, B. and Sand, A. (2021) 'The UK and digital trade: which way forward?', Blavatnik School Working Paper 2021/038

Keitner, C. I. and Clark, H. (2019). "Cybersecurity Provisions and Trade Agreements". 10 *Harv. Bus. L. Rev*. Online 1 (2019). Available at: https://repository.uchastings.edu/faculty_scholarship/1762

Kelsey, J. (2020). *DEPA lacks added value*. East Asia Forum. 10 April 2020. Available at: https://www.eastasiaforum.org/2020/04/10/depa-lacks-added-value/#more-245401

Leblond, P. (2020). *Digital Trade: Is RCEP the WTO's Future?* Centre for International Governance Innovation, 23 November 2020. Available at: https://www.cigionline.org/articles/digital-trade-rcep-wtos-future/

Leslie, D., Burr, C., Aitken, M., Cowls, J., Katell, M. and Brigg, M. (2021). *Artificial intelligence, human rights, democracy, and the rule of law - A primer*. The Alan Turing Institute. Published by the Council of Europe's Ad Hoc Committee on Artificial Intelligence. Available at: https://rm.coe.int/primer-en-new-cover-pages-coe-english-compressed-2754-7186-0228-v-1/1680a2fd4a

Liu, H. and Ching-Fu, L. (2020). "Artificial intelligence and global trade governance: a pluralist agenda." *Harvard International Law Journal*, Volume 61, Number 2, Summer 2020: 407-450.

Liu, J. (2020). "China's data localization". *Chinese Journal of Communication*, 13(1): 84-103.

López, D., Condon, B., and Muñoz, A. (2021). *Adapting to the Digital Trade Era: Challenges and opportunities*. Geneva: WTO, 2021. Chapter 10. pp. 214-228.

Lovelock, P. (2020). "Chapter 2: The New Generation of 'Digital' Trade Agreements: Fit for Purpose?". In Eduardo Pedrosa and Christopher Findlay, *State of the Region 2020*, 31–40. Available at: www.pecc.org/resources/regionalcooperation/2661-state-of-the-region-report-2020/file.

Malcolm, J. (2015). *Has the TPP Ended the Crypto Wars? Hardly*. Electronic Frontier Foundation. Available at: https://www.eff.org/deeplinks/2015/11/has-tpp-ended-crypto-wars

Manyika, J., Lund, S., Bughin, J., Woetzel, J., Stamenov, K. and Dhingra, D. (2016). *Digital Globalization: The New Era of Global Flows* (Washington: McKinsey Global Institute). Available at https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows

Marchant, G. E. (2011). "The growing gap between emerging technologies and the law". In G. E. Marchant *et al.* (eds.), *The growing gap between emerging technologies and legal-ethical oversight. The pacing problem* (New York: Springer).

Mattoo, A. and Meltzer, J. P. (2019). “International Data Flows and Privacy: The Conflict and Its Resolution”. *Journal of International Economic Law*, Volume 21, Issue 4, 769–789.

Mishra, N (2022). *Regulating artificial intelligence through digital trade agreements.* Hinrich Foundation. Available at: https://www.hinrichfoundation.com/research/wp/digital/regulating-artificial-intelligence-through-digital-trade-agreements/

Nan, Z. (2022). *China's accession to DEPA broadens opening-up in digital trade*. China Daily, 22 August 2022. Available at: https://www.chinadaily.com.cn/a/202208/22/WS63032deba310fd2b29e73927.html

Naef, T. (2023). "Restrictions on Data Transfers and Trade Agreements". In: *Data Protection without Data Protectionism. European Yearbook of International Economic Law*(), vol 28. Springer, Cham. https://doi.org/10.1007/978-3-031-19893-9_5

New Zealand Ministry of Foreign Affairs and Trade (2020a). *Digital Economy Partnership Agreement. National Interest Analysis*. June 2020. Available at: https://www.mfat.govt.nz/assets/Uploads/DEPA-NIA-June-2020.pdf

New Zealand Ministry of Foreign Affairs and Trade (2020b). *Digital Economy Partnership Agreement. Briefing for the Economic Development, Science and Innovation Committee, 2 July 2020*. Available at: https://www.mfat.govt.nz/assets/Trade-agreements/DEPA/Briefing-for-the-Economic-Development-Science-and-Innovation-Select-Committee-for-Parliamentary-Treaty-Examination.pdf

New Zealand Ministry of Foreign Affairs and Trade (n.d.). *Free Trade Agreement in Force - Trans-Pacific Strategic Economic Partnership (P4)*. Available at: https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/trans-pacific-strategic-economic-partnership-p4/

Organisation for Economic Co-operation and Development (OECD) (2020). *Mapping Approaches to data and data flows. Report for the G20 Digital Economy Task Force*. Available at: https://www.oecd.org/sti/mapping-approaches-to-data-and-data-flows.pdf

Organisation for Economic Co-operation and Development (OECD) (1997). *OECD Guidelines for Cryptography Policy*. Available at: https://www.oecd.org/sti/ieconomy/guidelinesforcryptographypolicy.htm

Organisation for Economic Cooperation and Development (OECD) (n.d.). *Digital Trade*. Available at: https://www.oecd.org/trade/topics/digital-trade/

Pasadilla, G. (2020). “Next generation nontariff measures: Emerging data policies and barriers to digital trade”. ARTNeT Working Paper Series No. 187, Asia-Pacific Research and Training Network on Trade (ARTNeT). Available at: https://artnet.unescap.org/publications/working-papers/next-generation-non-tariff-measures-emerging-data-policies-and-barriers

Pasadilla, G. (2020). “E-commerce provisions in RTAs: Implications for negotiations and capacity building”. ARTNeT Working Paper Series, No. 192, Asia-Pacific Research and Training Network on Trade (ARTNeT). Available at: https://www.econstor.eu/handle/10419/222464

Peng, S., Lin, C. and Streinz, T. (2021). "Artificial Intelligence and International Economic Law: A Research and Policy Agenda". In Shin-yi Peng, Ching-Fu Lin, and Thomas Streinz (eds), *Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration* (Cambridge: Cambridge University Press) Chapter 1.

Peters, M. A. (2022). "Digital trade, digital economy and the digital economy partnership agreement (DEPA)". *Educational Philosophy and Theory*, DOI: 10.1080/00131857.2022.2041413

Petri, P. A. and Plummer, M. G. (2020). "East Asia Decouples from the United States: Trade War, COVID-19, and East Asia's New Trade Blocs". Working Paper Series WP20-09, Peterson Institute for International Economics. Available at https://www.piie.com/sites/default/files/documents/wp20-9.pdf

Phillips, M. (2018). "International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR)". *Hum Genet*. 2018 Aug;137(8):575-582. doi: 10.1007/s00439-018-1919-7.

Ramasubramanian, G. (2020). *Building on the Modular Design of DEPA*. East Asia Forum, 10 July 2020. Available at: https://www.eastasiaforum.org/2020/07/10/building-on-the-modular-design-of-depa/

Reidenberg, J. (2000). "Resolving Conflicting International Data Privacy Rules in Cyberspace". *Stanford Law Review*, Vol. 52, No. 5, Symposium: Cyberspace and Privacy: A New LegalParadigm? (May, 2000), 1315-1371.

Soprana, M. (2021). "The Digital Economy Partnership Agreement (DEPA): Assessing the Significance of the New Trade Agreement on the Block". *Trade, Law and Development*, XIII. 143.

Subedi, S. P. (2008). *International investment law: Reconciling policy and principle* (Oxford and Portland, Oregon: Hart Publishing).

Undersecretariat of International Economic Relations of Chile (n.d.). *Acuerdos económico–comerciales vigentes, Chile-P4*. Available at: https://www.subrei.gob.cl/acuerdos-comerciales/acuerdos-comerciales-vigentes/p4

UNDP Global Centre for Technology, Innovation, and Sustainable Development (2021). *Enabling Cross-Border Data Flow: ASEAN and Beyond*. United Nations Development Programme (UNDP). Available at: https://www.undp.org/publications/enabling-cross-border-data-flow-asean-and-beyond

United Nations Conference on Trade and Development (UNCTAD) (2021). *Digital Economy Report 2021, Cross-border data flows and development: For whom the data flow*. United Nations Publications).

United Nations Conference on Trade and Development (UNCTAD) (2016). *Data protection regulations and international data flows: Implications for trade and development*. United Nations Publication.

Velli, F. (2019). 'The Issue of Data Protection in EU Trade Commitments: Cross-border Data Transfers in GATS and Bilateral Free Trade Agreements. *European papers: a journal on law and integration* Vol. 4, Nº. 3, 881-894

Viollier, P. (2019). *Digital Economy Partnership Agreement ¿Hacia dónde va el primer tratado sobe economía digital?* Derechos Digitales, 23 August 2019. Available at: https://www.derechosdigitales.org/13745/hacia-donde-va-el-primer-tratado-sobe-economia-digital/

Waitangi Tribunal (2023). *The Report on the Comprehensive and Progressive Agreement for Trans-Pacific Partnership* (Legislation Direct, Lower Hutt, New Zealand). Available at: https://forms.justice.govt.nz/search/Documents/WT/wt_DOC_195473606/Report%20on%20the%20CPTPP%20W.pdf

Wang, C. and Zhang, N. and Wang, Cong (2021). "Managing privacy in the digital economy". *Fundamental Research*, Volume 1, Issue 5, 543-551.

Wong, K. (2022). *China's bid to join digital economy pact hinges on clarification of data laws, experts say*. China Macro Economy, 27 August 2022. Available at: https://www.scmp.com/economy/china-economy/article/3190330/chinas-bid-join-digital-economy-pact-hinges-clarification

World Economy Forum (2020). *White Paper - Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows. Platform for Shaping the Future of Trade and Global Economic Interdependence*. Available at: https://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20_Flows_2020.pdf

Wunsch-Vincent, S. and Hold, A. (2012). "Towards coherent rules for digital trade: Building on efforts in multilateral versus preferential trade negotiations". In M. Burri and T. Cottier (eds.), *Trade Governance in the Digital Age: World Trade Forum* (pp. 179-221) (Cambridge: Cambridge University Press). doi:10.1017/CBO9781139136716.012

Xinzhen, L. (2022). *In DEPA Need of China*. China Focus, 2 September 2022. Available at: http://www.cnfocus.com/in-depa-need-of-china/

Yakovleva, S. and Irion, K. (2020a). "Pitching trade against privacy: reconciling EU governance of personal data flows with external trade". *International Data Privacy Law*, Volume 10, Issue 3, August 2020, 201–221

Yakovleva, S. and Irion, K. (2020b). "Toward Compatibility of the EU Trade Policy with the General Data Protection Regulation". *AJIL Unbound*, 114, 10-14

Yakovleva, S. (2020) "Privacy protection (ism): The latest wave of trade constraints on regulatory autonomy". 74 *U. Miami L. Rev.* 416.

Yoshimatsu, Hidetaka (2014). *Comparing Institution-Building in East Asia Power Politics, Governance, and Critical Junctures. Critical Studies of the Asia-Pacific* (Houndmills, Basingstoke, Hampshire: Palgrave Macmillan).

Zhou, C. (2021). *China applies to join digital trade pact with Singapore and NZ*. Nikkei Asia. Available at: https://asia.nikkei.com/Economy/Trade/China-applies-to-join-digital-trade-pact-with-Singapore-and-NZ