Scientific Research Publishing

Beijing Law Review, 2025, 16(2), 875-907
https://www.scirp.org/journal/blr
ISSN Online: 2159-4635
ISSN Print: 2159-4627

# Digital Sovereignty in Global Trade: Analysing WTO Governance of Data Flows

**Misbau Alamu Lateef**

The Law School, University of Hull, Hull, United Kingdom
Email: M.lateef@hull.ac.uk

**How to cite this paper:** Lateef, M. A. (2025). Digital Sovereignty in Global Trade: Analysing WTO Governance of Data Flows. *Beijing Law Review, 16,* 875-907.
https://doi.org/10.4236/blr.2025.162044

**Received:** March 21, 2025
**Accepted:** June 14, 2025
**Published:** June 17, 2025



## Abstract

This paper examines the evolving landscape of cross-border data flows within the international trade law framework, with a particular focus on the World Trade Organization's governance mechanisms. While digital trade and data transfers have become central to global commerce, the pre-internet WTO agreements present significant interpretative challenges in regulating these phenomena. Using doctrinal analysis, this paper critically assesses the application of GATT and GATS provisions to cross-border data flows, evaluates emerging regional approaches such as the RCEP and CPTPP, and examines the tension between trade liberalisation objectives and domestic policy priorities, including data privacy and digital sovereignty. The paper argues that while existing exceptions within WTO agreements potentially accommodate legitimate public policy objectives, the current fragmented regulatory approach creates legal uncertainty and risks undermining both free trade principles and legitimate regulatory interests. The paper contributes to scholarly discourse by proposing a balanced framework that reconciles trade facilitation with recognition of national regulatory autonomy in the digital sphere.

## Keywords

Digital Trade Governance, Cross-Border Data Flows, WTO Framework, Data Localisation, Digital Sovereignty, GATS, Regulatory Coherence, Trade Liberalisation

## 1. Introduction

The digital transformation of the global economy has altered the nature and scope of international trade in a fundamental way. Data flows across borders now constitute the backbone of the contemporary trading system, with the volume of cross-border data transfers growing exponentially year on year (Aaronson, 2016:

p. 17). The COVID-19 pandemic has further accelerated this digital transformation, as businesses and governments worldwide have increasingly relied on digital infrastructure to maintain economic activity amid physical restrictions (Dayday, 2023: p. 34). Today, cross-border data flows underpin virtually every aspect of international commerce—from supply chain management to financial services and from cloud computing to digital content delivery.

This transformation presents profound challenges for the international trade legal framework that was largely conceived and developed in the pre-digital era. The World Trade Organization (WTO) agreements, formulated in the early 1990s and brought into force in 1995, were negotiated at a time when the commercial internet was in its infancy, and the scale of contemporary digital trade was scarcely imaginable (Mitchell & Mishra, 2021: p. 83). The application of these 'pre-internet' agreements to digital phenomena has consequently become the subject of considerable legal and policy debate, with stakeholders from both developed and developing nations questioning whether the existing framework is fit for purpose in the digital age (Streinz, 2021).

Central to this debate is the question of how cross-border data flows should be governed within the international trade legal order. The issue is complicated by the multi-dimensional nature of data itself—simultaneously a tradeable commodity, an infrastructure for trade, and a repository of potentially sensitive personal, commercial, or governmental information (Burri, 2017a: pp. 410-413). This multifaceted character means that data governance inevitably intersects with a range of domestic policy priorities, including privacy protection, national security, digital industrial policy, and sovereign control over information (Casalini & González, 2019: p. 8). Reconciling these legitimate regulatory interests with the principles of trade liberalisation that underpin the WTO system presents significant conceptual and practical challenges.

In light of the foregoing, this paper examines how the international trade legal framework, with particular focus on the WTO agreements, can and should respond to the governance challenges posed by cross-border data flows. It explores the interpretative difficulties in applying existing GATT and GATS provisions to digital trade phenomena, evaluates emerging regional and plurilateral approaches to data governance in trade agreements, and proposes a balanced framework that recognises both the economic imperatives of digital trade liberalisation and the legitimate sovereign interests in regulating data flows.

The research methodology adopted by this paper is primarily doctrinal, focusing on the interpretation and application of legal texts, supplemented by limited comparative analysis of regional trade agreements and consideration of policy perspectives from both developed and developing economies. The paper draws on WTO jurisprudence, scholarly literature, and policy documents to develop a comprehensive understanding of the current legal landscape and potential pathways for reform.

The paper is divided into seven sections, including this introductory part and

others, as follows: Section II establishes a conceptual framework for understanding cross-border data flows and their relationship to international trade. Section III analyses the WTO legal framework and its application to digital trade, with particular focus on the classification challenges and interpretative questions that arise. Section IV examines regional trade agreements as laboratories for new approaches to data governance, comparing provisions in agreements such as the Regional Comprehensive Economic Partnership (RCEP) and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). Section V explores the balance between free trade principles and legitimate regulatory objectives, focusing on the role of exceptions within the WTO system. Section VI proposes elements of a harmonised approach to digital trade governance that could achieve greater regulatory coherence while respecting national policy autonomy. Finally, Section VII concludes with reflections on the future development of international trade law in the digital sphere.

Furthermore, this paper contributes to the scholarly discourse on international economic law by providing a systematic analysis of the application of WTO law to cross-border data flows, evaluating emerging approaches in preferential trade agreements, and proposing a balanced framework that could inform future negotiations on e-commerce within the WTO system. The analysis recognises that effective governance of cross-border data flows requires not only technical legal solutions but also a deeper appreciation of the sovereign interests at stake and the distributional implications of different regulatory approaches. By exploring these dimensions, the paper aims ultimately to advance understanding of how international trade law can adapt to the realities of the digital economy while accommodating legitimate diversity in national regulatory approaches.

## 2. Conceptual Framework: Digital Trade and Cross-Border Data Flows

### 2.1. Defining Cross-Border Data Flows and Their Economic Significance

To put it simply, cross-border data flows represent the movement of digital information across national boundaries (Burri, 2021: p. 11). This phenomenon encompasses a diverse range of activities—from the transmission of personal data in e-commerce transactions to the transfer of corporate information within multinational enterprises, from cloud computing services to digital content streaming, and from financial data transfers to real-time communication over telecommunications networks (Meltzer, 2014: p. 92). The common element in these varied contexts is the movement of machine-readable information across jurisdictional boundaries, typically via the internet infrastructure that has become fundamental to the contemporary global economy.

The economic significance of these data flows is profound and multifaceted. Research by the McKinsey Global Institute has estimated that cross-border data flows generated approximately $2.8 trillion in economic value in 2014, exceeding

the value of global trade in physical goods (Manyika et al., 2016: p. 23). This figure has undoubtedly grown substantially in subsequent years, particularly with the acceleration of digital transformation during the COVID-19 pandemic (Dayday, 2023: p. 34; Lateef & Akinsulore, 2021: pp. 7-8). Clearly, data flows contribute to economic growth through multiple channels: they enable international trade in digital services, enhance the efficiency of global value chains, facilitate innovation through knowledge transfer, create new business models and markets, and improve productivity through better resource allocation and decision-making (Casalini & González, 2019: pp. 11-12).

The economic value of data flows is not, however, evenly distributed across nations. Developed economies with advanced digital infrastructure, established technology sectors, and significant market power in the digital sphere have typically captured a disproportionate share of the benefits arising from the liberalisation of data flows (UNCTAD, 2021: p. 5). This asymmetry has raised concerns about digital dependency and digital colonialism, with developing nations apprehensive that unconstrained data flows may perpetuate or exacerbate existing economic inequalities (Gurumurthy, Vasudevan, & Chami, 2017).

### 2.2. Data as Both a Tradeable Commodity and Infrastructure for Trade

A key conceptual challenge in analysing cross-border data flows within the international trade legal framework is the dual nature of data as both a tradeable commodity and an infrastructure for trade (Dai, 2022: pp. 40-43). As a commodity, data can be bought, sold, and licensed across borders—exemplified by transactions involving databases, digital content, and various forms of information services. In this capacity, data resembles other tradeable goods and services, albeit with distinctive characteristics such as non-rivalry (multiple parties can use the same data simultaneously) and non-excludability (difficulties in preventing access and use once data is released) (Gervais, 2016: p. 10).

Simultaneously, data serves as an essential infrastructure for international trade across virtually all sectors. Digital information flows underpin global value chains, enable international financial transactions, facilitate cross-border service provision, and allow for the coordination of complex production processes across multiple jurisdictions (Aaronson, 2019: p. 543). In this infrastructural role, data is less a direct object of trade than a medium through which trade occurs—something similar to transport networks or communication systems, but with distinct characteristics deriving from its intangible, replicable nature.

This dual character complicates the application of traditional trade law categories, which typically distinguish between goods and services and between traded items and the infrastructure enabling trade. When data flows across borders as part of an e-commerce transaction, is it being traded as a commodity, serving as infrastructure for trade, or both? The answer has significant implications for the applicable legal regime, as examined in detail in Section III below.

### 2.3. Digital Sovereignty and the Competing Interests in Data Governance

The concept of digital sovereignty has emerged as a central organising principle for the approaches of many nations to data governance (Chander & Lê, 2015: pp. 680-681). Digital sovereignty encompasses a state's claim to exercise authority over data related to its territory, citizens, and economic activities, thereby reflecting traditional notions of sovereignty adapted to the digital context. This concept manifests differently across jurisdictions: from the European emphasis on regulatory sovereignty through comprehensive data protection frameworks to China's focus on territorial data sovereignty through localisation requirements to the American prioritisation of commercial sovereignty through market-oriented approaches (Farrell & Newman, 2019: pp. 57-62).

The assertion of digital sovereignty through data regulation responds to multiple legitimate state interests. Privacy protection has perhaps been most prominent, exemplified by the European Union's General Data Protection Regulation (GDPR), which imposes restrictions on cross-border transfers of personal data to jurisdictions lacking 'adequate' protection (GDPR, 2016: Ch V). National security concerns have similarly motivated constraints on data flows, particularly for sensitive information related to government operations, critical infrastructure, and defence (Wang, 2020: p. 119). Economic development objectives have also shaped data governance approaches, with some states adopting localisation requirements as a form of digital industrial policy designed to promote domestic data processing industries (Ferracane, 2017: pp. 7-8).

However, these sovereign interests often appear to conflict with the trade liberalisation principles that underpin the WTO system, creating tension between the economic logic of free data flows and the political logic of sovereign control (Yakovleva & Irion, 2020: p. 204). Yet, this apparent conflict may be overstated—effective data governance can enhance rather than undermine the benefits of digital trade by building trust, establishing interoperability, and providing the regulatory certainty necessary for sustainable economic development (OECD, 2019: p. 5). The challenge for the international trade legal framework is to accommodate legitimate expressions of digital sovereignty while preventing protectionist and/or predatory measures disguised as regulatory policy.

### 2.4. The Evolving Nature of Digital Trade and Regulatory Responses

Digital trade is a rapidly evolving phenomenon, characterised by continuous technological innovation and the emergence of new business models. From the early days of e-commerce focused on tangible goods, digital trade has expanded to encompass complex service offerings, platform-based business models, data-driven technologies like artificial intelligence, and novel forms of digital assets (WTO, 2020: pp. 56-63). This evolution has been accompanied by changes in the nature and scale of cross-border data flows, from relatively simple client-server commu-

nications to the massive, continuous data transfers that characterise contemporary cloud computing and IoT applications (International Organization for Standardization, 2016).

Regulatory responses to digital trade have similarly evolved, though typically lagging behind technological and market developments. The initial regulatory approach often emphasised non-intervention to allow digital markets to develop, exemplified by the 1998 WTO Declaration on Global Electronic Commerce establishing a temporary moratorium on customs duties for electronic transmissions (WTO Ministerial Conference, 1998). As digital markets matured and concerns about their social, economic, and political implications grew, more interventionist approaches emerged—from data protection regulations to digital service taxes, from competition interventions to content moderation requirements (OECD, 2019).

The relationship between technological evolution and regulatory response creates a dynamic environment for international trade law. New technologies and business models continually challenge existing legal categories and regulatory frameworks, while regulatory innovations, in turn, shape the development of digital markets (Lemley, 1998). This dynamic interaction underscores the need for an adaptive international legal framework that can accommodate technological change while providing sufficient certainty for businesses and governments.

The foregoing analysis has established the conceptual framework underlying the thesis of this paper, and the following section examines how the WTO legal system currently applies to cross-border data flows, identifying both the challenges in interpreting 'pre-internet' agreements in the digital context and the potential pathways for addressing these challenges within the existing legal architecture.

## 3. The WTO Framework and Its Application to Cross-Border Data Flows

### 3.1. Origins and Limitations of the WTO Agreements in Digital Governance

The World Trade Organization agreements were negotiated during the Uruguay Round of trade talks from 1986 to 1994 and came into force on 1 January 1995 (Marrakesh Agreement Establishing the World Trade Organization, 1994). This timing is significant for understanding the limitations of the WTO framework in governing digital trade: the agreements were concluded just as the commercial internet was beginning to emerge but before its transformative economic impact could be anticipated. As Dayday notes, "international trade law and the agreements forming the World Trade Organization (WTO) do not explicitly regulate digital trade and its different aspects, including cross-border data flows and data localization" (Dayday, 2023: p. 33).

The WTO framework was designed primarily to address the trade challenges of the late 20th century—focusing on reducing tariffs on physical goods, opening markets for services through traditional modes of supply, and protecting intellectual property in conventional forms. The agreements reflect what might be termed

a "pre-internet state" (Burri, 2017a: p. 3), lacking specific provisions tailored to the distinctive characteristics of digital trade and cross-border data flows. This creates what Mitchell and Mishra have described as an "interpretative technological translation" problem—the challenge of applying rules framed for an analog world to digital phenomena (Mitchell & Mishra, 2021: p. 93; Wu, 2006: p. 264).

The limitations of the WTO framework in addressing digital trade are particularly apparent in three areas. First, the agreements lack specific provisions on cross-border data flows, data localisation requirements, or digital services regulation. Second, the classification system underpinning the agreements—particularly the distinction between goods and services—struggles to accommodate the hybrid nature of many digital products and services. Third, the sectoral classifications used in the GATS commitments of members reflect a pre-digital economy, making it difficult to determine how commitments apply to novel digital services (Dai, 2022: pp. 49-50).

Despite these limitations, the WTO has recognised the growing importance of digital trade. In 1998, the Second Ministerial Conference adopted the Declaration on Global Electronic Commerce, establishing a temporary moratorium on customs duties for electronic transmissions and creating a Work Programme on Electronic Commerce (WTO Ministerial Conference, 1998). This Work Programme has served as a forum for discussing digital trade issues but has not led to substantive new agreements, with members divided on fundamental questions about the application of existing rules to digital phenomena.

### 3.2. GATT Provisions and Their Applicability to Data as Goods

The General Agreement on Tariffs and Trade (GATT) governs international trade in goods, establishing rules on tariffs, non-discrimination, quantitative restrictions, and exceptions to these obligations. As noted earlier, a threshold question in applying the GATT to cross-border data flows is whether data constitutes a "good" within the meaning of the agreement.

Several arguments support treating data as a good under the GATT. Data has value, can be owned (through intellectual property rights), and can be exchanged between parties (Dai, 2022: pp. 40-42). Digital content, such as e-books, software, and digital media, shares many characteristics with physical goods that unquestionably fall within the GATT's scope. Moreover, the WTO Appellate Body has previously recognised that electronically delivered content can be classified as a good, as in China—Publications and Audiovisual Products case, where it held that electronic distribution of audio-visual content fell within China's GATT commitments (World Trade Organization, 2010: para 377).

However, counterarguments suggest that data may fall outside the GATT's scope. The ordinary meaning of "goods" arguably implies tangibility, which data lacks. The negotiating history of the GATT reveals no contemplation of intangible products like data. Furthermore, the existence of the GATS, which explicitly covers services delivered electronically, could suggest that electronic transmissions

were intended to be regulated as services rather than goods (Mitchell & Hepburn, 2018: pp. 196-197).

If data is classified as "goods" under the GATT, several key provisions would apply to cross-border data flows. Article I would require members to extend the Most-Favoured-Nation (MFN) treatment to data flows from all WTO members. Article III would prohibit discrimination between domestic and imported data (national treatment). Article XI would prohibit quantitative restrictions on data imports and exports, potentially capturing data localisation requirements and prohibitions on data exports. Articles XX and XXI would provide exceptions for measures necessary to protect public morals, human health, and essential security interests, among other objectives.

The application of these provisions to data flows remains largely theoretical, as no WTO dispute has directly addressed the question of whether or not data constitutes goods. Nevertheless, the expansion of digital trade increases the likelihood that such questions will eventually require authoritative resolution, whether through dispute settlement or negotiated clarification among members.

### 3.3. GATS Framework and Challenges in Classification of Digital Services

The General Agreement on Trade in Services (GATS) provides a more promising framework for addressing cross-border data flows, as many digital activities clearly constitute services. The GATS categorises services according to four modes of supply: Mode 1 (cross-border supply), Mode 2 (consumption abroad), Mode 3 (commercial presence), and Mode 4 (presence of natural persons) (GATS, 1995: Art I: 2). Cross-border data flows most naturally fall within Mode 1, where "the service crosses the border" without the movement of persons (GATS, 1995: Art I: 2(a)).

However, classifying digital services under the GATS presents several challenges. First, many digital services were not contemplated when members made their initial GATS commitments in the 1990s, creating uncertainty about the applicable obligations. Second, digital services often blur the boundaries between established service categories. For example, does a cloud storage service constitute a computer service, a telecommunications service, or a data processing service? (Mitchell & Hepburn, 2018: p. 198). Third, the distinction between modes of supply becomes ambiguous in the digital context—Is a consumer who accesses a foreign website receiving a cross-border service (Mode 1) or consuming a service abroad (Mode 2)? (Dai, 2022: p. 48)

These classification challenges notwithstanding, the Appellate Body has confirmed that the GATS applies to electronically delivered services. In the US, Gambling held that online gambling services fell within the scope of "recreational services" in US commitments despite being delivered through technology not contemplated during the Uruguay Round (World Trade Organization, 2005: paras 180-181). This reasoning suggests that existing GATS commitments extend to services delivered through new technologies, including those involving cross-border

data flows.

A related challenge concerns the scope of members' commitments regarding digital services. Under the GATS, liberalization commitments are made on a sector-by-sector basis, with members specifying which services they will open to foreign competition and under what conditions. Most members made commitments based on the WTO Services Sectoral Classification List (W/120), which was developed before many digital services existed (WTO, 1991). Consequently, there is considerable disagreement about how digital services map onto these commitments—does a search engine fall under computer services, telecommunications services, or advertising services? The answer determines which GATS obligations apply to measures affecting the service.

Assuming that a digital service falls within the scope of a member's commitments, several GATS provisions become relevant to cross-border data flows. Most fundamentally, Article XVI (Market Access) prohibits quantitative restrictions on services, which could encompass data localization requirements that effectively limit the number of service suppliers (GATS, 1995: Art XVI: 2). Article XVII (National Treatment) prohibits discrimination against foreign services and service suppliers, potentially capturing regulations that treat foreign data services less favourably than domestic ones (GATS, 1995: Art XVII: 1).

### 3.4. The Telecommunications Annex and Cross-Border Information Transfers

The GATS Annex on Telecommunications provides perhaps the most explicit reference to cross-border data flows in the WTO agreements. Article 5(c) of the Annex requires members to ensure that service suppliers may use public telecommunications networks for "the movement of information within and across borders" and for "access to the information contained in databases or otherwise stored in machine-readable form in the territory of any Member" (GATS, 1995: Annex on Telecommunications, para 5(c)). This provision creates an obligation to allow information to flow across borders through telecommunications networks, which would encompass many forms of data transfer.

However, the scope of this obligation is limited in several respects. It applies only to information transferred through "public telecommunications transport networks and services," potentially excluding data flows through private networks (GATS, 1995: Annex on Telecommunications, para 5(c)). It benefits only "service suppliers" using telecommunications to provide services listed in members' schedules, not all data transfers. It also requires access to information only "for the supply of a service included in [a member's] Schedule," not for all purposes (GATS, 1995: Annex on Telecommunications, para 5(c)).

Despite these limitations, the Telecommunications Annex demonstrates that the drafters of the WTO agreements recognised the importance of cross-border information flows to trade in services. As Mitchell and Hepburn observe, "the provision implies that restrictions on the cross-border flow of data or the storage

of data outside a Member's territory could potentially prevent access to information necessary for the supply of a scheduled service in violation of Article 5(c)" (Mitchell & Hepburn, 2018: p. 196). This suggests that the Annex could serve as a basis for challenging some forms of data flow restrictions or localization requirements.

### 3.5. WTO Jurisprudence and Interpretative Approaches

While no WTO dispute has directly addressed cross-border data flows, several cases provide guidance on how the agreements might apply in the digital context. These cases reveal an evolutionary approach to interpretation, with the Appellate Body recognizing that the WTO agreements must adapt to technological and commercial developments.

In China—Publications and Audiovisual Products, the Appellate Body held that China's GATT commitments on the right to trade covered electronic distribution of audiovisual products, despite this form of distribution not existing when the commitments were made (World Trade Organization, 2010: para 396). The Appellate Body emphasized that treaty terms can evolve over time and should be interpreted in light of contemporary technological realities.

Similarly, in US—Gambling, the Appellate Body found that online gambling services fell within the scope of US commitments on "recreational services," even though internet gambling was not significant when these commitments were made (World Trade Organization, 2005: para 177). The Appellate Body rejected a narrow interpretation tied to the technological context of the Uruguay Round, instead adopting an approach that allowed the GATS to accommodate technological evolution.

These cases suggest that the WTO dispute settlement body would likely adopt a technologically neutral, evolutionary approach to interpreting the agreements in relation to digital trade. Such an approach would recognise that commitments made concerning traditional goods and services extend to their digital counterparts, even if the digital forms were not contemplated during the Uruguay Round. This interpretative flexibility provides a partial solution to the "pre-internet" limitations of the WTO agreements.

Nevertheless, jurisprudential evolution can only go so far in addressing the governance challenges posed by cross-border data flows. As Dayday observes, "While there have been attempts to fit digital trade in the current scheme of WTO law, these are not entirely conclusive" (Dayday, 2023: p. 33). The fundamental limitations of agreements negotiated before the digital revolution create inherent constraints on their application to novel digital phenomena. This reality has prompted members to explore new approaches through regional trade agreements, as examined in the following section.

## 4. Regional Trade Agreements as Regulatory Laboratories

### 4.1. The Emergence of Data Provisions in Modern Trade Agreements

As the limitations of the WTO framework in addressing digital trade have become

increasingly apparent, countries have turned to regional and bilateral free trade agreements (FTAs) to establish rules governing cross-border data flows. These agreements have emerged as important regulatory laboratories where countries experiment with new approaches to digital trade governance, potentially establishing templates for future multilateral rules (Burri, 2017b: p. 95). The proliferation of digital trade provisions in FTAs thus reflects what Burri describes as "a definite shift from the multilateral level of rule-making to preferential venues" (Burri, 2021: p. 19).

This shift gained momentum in the early 2010s when countries began incorporating dedicated e-commerce chapters into their trade agreements. According to a dataset compiled by Burri and colleagues, 184 FTAs now contain provisions related to digital trade, with most negotiated within the last decade (Burri et al., 2022). These provisions range from basic commitments to promote e-commerce cooperation to sophisticated rules on cross-border data flows, data localization, and digital customs duties. The content and ambition of these provisions vary considerably, reflecting the diverse and sometimes conflicting approaches to digital governance among trading nations.

The emergence of data provisions in FTAs represents a response to both economic and regulatory imperatives. Economically, countries seek to capture the benefits of digital trade by reducing barriers to cross-border data flows and establishing predictable rules for digital businesses. Regulatorily, they aim to preserve policy space for legitimate public objectives while preventing disguised protectionism in the digital sphere. The resulting agreements reflect negotiations between these sometimes-competing objectives, with outcomes shaped by the relative economic and negotiating power of the parties involved.

### 4.2. Comparative Analysis of RCEP and CPTPP Approaches to Data Flows

The Regional Comprehensive Economic Partnership (RCEP) and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) represent two of the most significant recent FTAs containing provisions on cross-border data flows. Both agreements include dedicated e-commerce chapters with rules on data flows and localization, but they differ markedly in their approach and level of ambition, providing useful contrasts for comparative analysis.

The CPTPP, which evolved from the Trans-Pacific Partnership following U.S. withdrawal, establishes relatively strong disciplines on data flows and localization. Article 14.11 states that "Each Party shall allow the cross-border transfer of information by electronic means...when this activity is for the conduct of the business of a covered person" (CPTPP, 2018: Art 14.11 (2)). This obligation explicitly includes personal information, addressing a key category of data subject to restrictive regulations. Similarly, Article 14.13 prohibits requirements to "use or locate computing facilities in that Party's territory as a condition for conducting business in that territory" (CPTPP, 2018: Art 14.13 (2)). These provisions aim to prevent

data localisation measures and restrictions on cross-border data flows, promoting an open digital trading environment.

The RCEP adopts a more qualified approach. While it contains similar baseline obligations on data flows and localisation in Articles 12.15 and 12.14, respectively, these are subject to broader exceptions. The agreement recognises each party's right to regulate legitimate public policy objectives and explicitly states that "the necessity behind the implementation of such legitimate public policy shall be decided by the implementing Party" (RCEP, 2020: Art 12.15 (3) (a) fn 14). Moreover, RCEP includes a self-judging security exception, stating that measures protecting "essential security interests...shall not be disputed by other Parties" (RCEP, 2020: Art 12.14 (3) (b)). These provisions preserve significantly more regulatory autonomy for parties than the CPTPP approach.

The differences between the CPTPP and RCEP reflect the diverse membership of the two agreements. The CPTPP includes countries with generally liberal approaches to digital trade, such as Japan, Singapore, and Canada, who favour stronger disciplines on data flow restrictions. The RCEP, by contrast, encompasses countries with varying approaches to digital governance, which maintains extensive data localisation requirements and restrictions on cross-border flows. The more flexible RCEP provisions represent a compromise between these divergent regulatory philosophies, preserving space for diverse national approaches while establishing baseline principles against discriminatory measures.

Both agreements also differ in their treatment of privacy and data protection. The CPTPP requires parties to "adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce" but does not establish minimum standards for this protection (CPTPP, 2018: Art 14.8 (2)). It also encourages the development of mechanisms to promote compatibility between different data protection regimes. The RCEP contains similar provisions but with even less prescription, simply requiring parties to adopt "legal, regulatory, and administrative provisions" for personal information protection without specifying their nature or scope (RCEP, 2020: Art 12.8 (1)).

### 4.3. Relative Strengths and Weaknesses of Regional Approaches

However, the proliferation of data provisions in regional trade agreements offers several advantages over the current WTO approach. Most obviously, these agreements provide explicit rules tailored to digital trade, addressing the absence of specific provisions in the WTO texts. They respond to technological and commercial developments that have occurred since the conclusion of the Uruguay Round, establishing frameworks better adapted to contemporary digital realities. Moreover, the regional approach allows for experimentation with different regulatory models, generating evidence about the effects of various provisions that can inform future negotiations.

Regional agreements can also better accommodate the legitimate diversity in national approaches to digital governance. The RCEP model, with its emphasis on

regulatory autonomy, allows countries with different values and priorities to cooperate on digital trade while preserving their distinctive regulatory approaches. As Streinz observes, the RCEP represents "a new attempt to reconcile the technological potential and economic rationale for digital interconnectivity with countries' ability to regulate their increasingly digital economies and societies" (Streinz, 2021: p. 2).

However, the regional approach also presents significant limitations. The proliferation of different rules across agreements creates a "spaghetti bowl" effect of sorts, where businesses operating across multiple jurisdictions must navigate diverse and sometimes conflicting requirements (Bhagwati, 1995: p. 4). This regulatory fragmentation increases compliance costs, particularly for small and medium enterprises with limited resources for legal analysis. It also potentially undermines the economic benefits of digital trade liberalisation by preserving regulatory barriers between different trade agreement zones.

More fundamentally, regional approaches risk perpetuating or exacerbating global digital divides. Developing countries with limited negotiating capacity may accept provisions in bilateral agreements with powerful trading partners that they would not agree to in multilateral settings where they can form coalitions (Drahos, 2002: p. 784). The resulting agreements may disproportionately benefit companies from developed economies with established digital advantages while constraining policy space for digital development strategies in less advanced economies. As the UNCTAD Digital Economy Report 2021 warns, "any outcome of the negotiations will mainly reflect the interests of companies in more advanced economies, which are currently the best positioned to capture value from the expansion of data flows" (UNCTAD, 2021: p. 145).

### 4.4. Implications for Multilateral Governance at the WTO Level

The developments in regional trade agreements have significant implications for multilateral digital trade governance through the WTO. Most directly, provisions in regional agreements serve as potential templates for WTO rules, with successful approaches potentially scaling up to the multilateral level. The ongoing Joint Statement Initiative (JSI) on E-commerce, launched by 76 WTO members at the 2017 Buenos Aires Ministerial Conference, draws inspiration from provisions tested in regional contexts (WTO, 2019). The JSI aims to develop rules on digital trade issues, including cross-border data flows, suggesting that regional experimentation may indeed feed into multilateral outcomes.

Regional agreements also create competitive pressure for multilateral progress. As more countries commit to binding disciplines on digital trade through FTAs, the opportunity cost of WTO inaction increases. Members excluded from regional arrangements may push for multilateral rules to avoid discriminatory treatment, while those already participating in ambitious FTAs may seek to multilateralise their preferred approaches. This dynamic potentially increases the constituency for WTO reform on digital issues, though significant divisions remain on the ap-

propriate content and scope of such reform.

The relationship between regional and multilateral approaches raises important systemic questions about the future of the trading system. One possibility is that regional agreements serve as building blocks for eventual multilateral convergence, with successful provisions gradually incorporated into the WTO framework. Alternatively, regional approaches could become permanent alternatives to multilateral governance, with digital trade regulated primarily through a network of overlapping FTAs. The outcome will depend largely on whether WTO members can overcome their differences on fundamental issues of digital governance—from the classification of digital products to the balance between liberalization and regulatory autonomy.

In the interim, the co-existence of regional and multilateral rules creates complex legal questions about their interaction. Most FTAs include provisions specifying that they do not derogate from WTO obligations, but interpretative challenges arise when applying both sets of rules to digital measures. For example, if a data localisation requirement violates CPTPP obligations but is justified under GATS exceptions, which assessment prevails? These questions become particularly acute in dispute settlement, where adjudicators must navigate the relationship between different legal regimes in an area of rapidly evolving state practice.

The next section examines how these various legal frameworks balance the competing objectives of trade liberalisation and legitimate regulatory interests, focusing on the role of exception provisions in accommodating public policy objectives in the digital sphere.

## 5. Balancing Free Trade and Legitimate Regulatory Objectives

### 5.1. The Relationship between Data Privacy Regulations and Trade Obligations

Data privacy regulations present one of the most significant tensions between free trade principles and legitimate regulatory objectives in the digital sphere. Privacy protection is recognised globally as a fundamental right and legitimate policy objective (Universal Declaration of Human Rights, 1948: Art 12; International Covenant on Civil and Political Rights, 1966: Art 17), yet privacy regulations often restrict cross-border data flows in ways that potentially conflict with trade liberalisation commitments. This tension manifests across multiple jurisdictions but is perhaps most evident in the European Union's General Data Protection Regulation (GDPR), which limits transfers of personal data to countries lacking "adequate" protection (GDPR, Arts 44-50).

The relationship between privacy regulations and trade obligations varies across the international legal framework. Under the WTO agreements, Article XIV(c)(ii) of the GATS contains a specific exception for measures necessary to secure "the protection of the privacy of individuals in relation to the processing and dissemination of personal data" (GATS, 1995: Art XIV (c) (ii)). This excep-

tion explicitly recognises privacy protection as a legitimate basis for deviating from GATS commitments, though subject to the requirement that measures are "necessary" and not "arbitrary or unjustifiable discrimination" or a "disguised restriction on trade" (GATS, 1995: Art XIV chapeau).

The approach in regional trade agreements has evolved toward more explicit accommodation of privacy regulations. Earlier agreements often contained minimal references to privacy, but recent agreements like the CPTPP and RCEP include specific provisions recognising the importance of data protection while encouraging interoperability between different regimes (CPTPP, 2018: Art 14.8; RCEP, 2020: Art 12.8). The CPTPP acknowledges that each party may "have its own regulatory requirements concerning the transfer of information by electronic means," while the RCEP explicitly permits measures necessary to ensure "data security and confidentiality of specific information of users" (CPTPP, 2018: Art 14.11 (1); RCEP, 2020: Art 12.14 (1)).

These provisions reflect a growing recognition that effective privacy protection can complement rather than undermine digital trade by building consumer trust and establishing consistent rules. As Yakovleva and Irion argue, "privacy and data protection laws could spur innovation by prompting the development and wider use of technologies based on anonymization and differential privacy algorithms, so that less personal data are involved in international transfers" (Yakovleva & Irion, 2016: pp. 206-207). From this perspective, the relationship between privacy regulations and trade obligations is not inherently antagonistic, provided that privacy measures are designed to achieve legitimate objectives rather than disguised protectionism.

Nevertheless, significant challenges remain in reconciling diverse privacy regimes with trade liberalisation objectives. Countries differ markedly in their conceptual approaches to privacy—from rights-based regimes like the GDPR to sectoral approaches like the U.S. framework to security-oriented models in countries like China and Russia (Greenleaf, 2021: p. 1). These differences reflect legitimate variations in societal values and institutional contexts but create substantial barriers to cross-border data flows and regulatory interoperability. The international trade legal framework must navigate this diversity while preserving both meaningful privacy protection and the benefits of digital trade.

### 5.2. National Security Exceptions and Their Applicability to Data Governance

National security has emerged as another critical area where legitimate regulatory interests potentially conflict with digital trade liberalisation. Countries now increasingly view data governance as a security issue, reflecting the strategic importance of data for economic competitiveness, critical infrastructure, defence capabilities, and societal resilience (Farrell & Newman, 2019: pp. 45-50). This security dimension manifests in various data governance measures, from localisation requirements for critical data to restrictions on transfers to jurisdictions unilater-

ally deemed security risks.

The WTO agreements recognise national security as a legitimate basis for deviating from trade commitments through the general exceptions in GATT Article XXI and GATS Article XIV bis (GATT, 1994: Art XXI; GATS, 1995: Art XIV bis). These provisions permit members to take measures they consider "necessary for the protection of [their] essential security interests," particularly those "relating to the supply of services as carried out directly or indirectly for the purpose of provisioning a military establishment" or "taken in time of war or other emergency in international relations" (GATS, 1995: Art XIV bis(b)).

The interpretation of security exceptions has traditionally been highly deferential to members' own assessments, but the Russia—Traffic in Transit case established that these exceptions are not entirely self-judging (World Trade Organization, 2019: para 7.102). The panel held that while members have discretion to define their essential security interests, their invocation of security exceptions must be made in good faith and meet minimum standards of plausibility (World Trade Organization, 2019: para 7.132). This holding potentially constrains the use of security exceptions to justify digital protectionism disguised as security measures.

Regional trade agreements have adopted varying approaches to security exceptions in the digital context. The CPTPP follows the traditional WTO language on essential security interests, while the RCEP adopts a more deferential approach, explicitly stating that security measures "shall not be disputed by other Parties" (RCEP, 2020: Art 12.14 (3) (b)). This variance reflects differing perspectives on the appropriate balance between security sovereignty and trade disciplines, with significant implications for data governance.

The security dimension of data governance raises complex questions for international trade law. How should adjudicators distinguish genuine security measures from disguised digital protectionism? What degree of deference should be afforded to national security assessments in the highly technical domain of data governance? How can the trading system accommodate legitimate security interests while preventing their abuse to justify restrictive data policies? These questions will likely occupy a central place in future developments at both the regional and multilateral levels.

### 5.3. Public Morals and Public Order Exceptions under WTO Law

Beyond privacy and security, WTO law recognises several other grounds for deviating from trade commitments that are relevant to data governance. Most importantly, GATT Article XX(a) and GATS Article XIV(a) permit measures "necessary to protect public morals" or "to maintain public order" (GATT, 1994: Art XX (a); GATS, 1995: Art XIV (a)). These broadly framed exceptions have been interpreted to encompass diverse societal values and have featured prominently in digital trade disputes.

In US—Gambling, the Appellate Body defined "public morals" as "standards of right and wrong conduct maintained by or on behalf of a community or nation"

(World Trade Organization, 2005: para 296). It accorded substantial deference to members in defining their own public morals, recognising that these standards "can vary in time and space, depending upon a range of factors, including prevailing social, cultural, ethical and religious values" (World Trade Organization, 2005: para 296). Similarly, the concept of "public order" has been interpreted broadly to refer to "the preservation of the fundamental interests of a society, as reflected in public policy and law" (World Trade Organization, 2005: para 296 fn 193).

These exceptions provide significant flexibility for WTO members to regulate digital content and services based on societal values. Countries have invoked public morals to justify restrictions on gambling services, measures against pornography, and regulations concerning politically sensitive content. The broad interpretation of these concepts gives members substantial policy space to regulate the digital sphere according to their distinctive moral and cultural perspectives.

However, public morals and public order exceptions are subject to a necessity test, requiring that measures be genuinely aimed at protecting these interests and not more trade restrictive than necessary to achieve their objectives (World Trade Organization, 2001: para 162). This test involves weighing and balancing several factors: the importance of the interest protected, the contribution of the measure to that objective, and the trade restrictiveness of the measure, considering available alternatives (World Trade Organization, 2001: para 164). This analysis allows adjudicators to distinguish legitimate moral regulation from disguised protectionism.

In the context of data governance, public morals, and public order exceptions could potentially justify various measures affecting cross-border data flows—from content filtering to requirements that certain sensitive data be processed domestically. The viability of such justifications would depend on demonstrating a genuine connection to moral or public order objectives and showing that the measures were not more trade-restrictive than necessary. This assessment would likely be highly context-specific, considering the particular societal values at stake and the technical details of the challenged measures.

### 5.4. The Necessity Test and Proportionality in Data Regulation

The "necessity test" found in many WTO exceptions serves as a crucial mechanism for balancing trade liberalisation with legitimate regulatory objectives. This test appears in both GATT Article XX and GATS Article XIV, requiring that measures be "necessary" to achieve objectives like protecting public morals, human health, or privacy (GATT, 1994: Art XX (a), (b), (d); GATS, 1995: Art XIV (a), (b), (c)). The test has been interpreted to involve a relational analysis between the measure, its objective, and its trade restrictiveness, incorporating elements of proportionality review.

In Korea—Various Measures on Beef, the Appellate Body established that necessity involves "a process of weighing and balancing a series of factors," including "the contribution made by the compliance measure to the enforcement of the law or regulation at issue, the importance of the common interests or values protected

by that law or regulation, and the accompanying impact of the law or regulation on imports or exports" (World Trade Organization, 2001: para 164). This analysis essentially asks whether the trade restrictiveness of a measure is proportionate to its contribution to a legitimate regulatory objective, considering the importance of that objective.

The necessity test plays a particularly important role in evaluating data governance measures, given the varied and sometimes conflicting objectives that such measures may serve. For example, data localization requirements might be justified as necessary for privacy protection or security, but their trade restrictiveness must be proportionate to their contribution to these objectives. If less trade-restrictive alternatives—such as contractual safeguards or certification mechanisms—could achieve the same level of protection, the localisation requirement might fail the necessity test.

Regional trade agreements have adapted and refined the necessity of analysis in the digital context. The CPTPP requires that measures affecting cross-border data flow "not impose restrictions...greater than are required to achieve the objective" (CPTPP, 2018: Arts 14.11 (3) (b), 14.13 (3) (b)), while the RCEP gives parties greater discretion to determine the necessity of their measures. These varying approaches reflect differing perspectives on the appropriate balance between regulatory autonomy and disciplines on digital protectionism.

The necessity test has been criticized from both liberalization and regulatory perspectives. Advocates of free data flows argue that the test gives excessive deference to domestic regulators, allowing measures that unnecessarily restrict trade, while advocates of regulatory autonomy contend that the test unduly constrains legitimate policy choices by imposing external standards of necessity (Trachtman, 1999: p. 346). These critiques highlight the inherent tension in balancing sovereign regulatory interests with the disciplines of a rules-based trading system.

### 5.5. Developing a Coherent Balancing Framework

The proliferation of data governance measures and their intersection with trade obligations calls for a coherent framework that can balance legitimate regulatory objectives with trade liberalization principles. Such a framework would need to accommodate the multidimensional nature of data —as both a tradeable commodity and a repository of sensitive information with implications for privacy, security, and sovereignty. It would also need to navigate the tensions between harmonisation and regulatory diversity, recognising both the benefits of interoperability and the legitimacy of different regulatory approaches.

Several principles could inform such a balancing framework. First, regulatory transparency should be emphasized, with measures affecting data flows clearly articulated and communicated to trading partners and stakeholders. Second, the principle of non-discrimination should apply, with measures avoiding arbitrary distinctions between domestic and foreign data or service providers. Third, proportionality should guide regulatory design, ensuring that measures are tailored

to their objectives and not more trade restrictive than necessary. Fourth, interoperability should be prioritized where possible, with mechanisms for recognizing equivalent protections across different regulatory systems.

These principles would not eliminate all tensions between data regulation and trade obligations, but they could help manage these tensions in a manner that preserves both meaningful regulatory autonomy and the benefits of digital trade integration. By establishing a common vocabulary and analytical framework, they could also facilitate more productive negotiations on digital trade rules at both regional and multilateral levels.

The development of such a balancing framework is not merely a technical exercise but a fundamentally political one involving choices about the relative priority of different values and interests. These choices cannot be resolved through legal analysis alone but require inclusive dialogue among stakeholders with diverse perspectives on the proper balance between digital sovereignty and global integration. The next section explores potential pathways for achieving greater coherence in digital trade governance while accommodating this legitimate diversity of approaches.

## 6. Towards a Harmonized Framework for Digital Trade Governance

### 6.1. Models for Regulatory Cooperation in Data Governance

The fragmentation of approaches to data governance across jurisdictions has generated substantial compliance costs for businesses operating globally and uncertainty about the rules governing cross-border data flows. This situation has prompted the exploration of various models for regulatory cooperation that could reduce friction while respecting legitimate regulatory diversity. Several approaches have emerged, each with distinctive features and implications for the balance between harmonisation and regulatory autonomy (Mitchell & Mishra, 2018: p. 1111).

The equivalence or adequacy model, exemplified by the EU's approach under the GDPR, involves unilateral determinations that another jurisdiction's legal framework provides protection equivalent to or adequate to the evaluating jurisdiction's standards (GDPR, 2016: Art 45). This approach preserves the regulatory autonomy of the evaluating jurisdiction while potentially facilitating data flows with jurisdictions meeting its standards. However, it has been criticised for its asymmetry—the evaluating jurisdiction imposes its standards without reciprocal obligations—and for the political dimensions of adequacy decisions, which may reflect strategic considerations beyond purely technical assessments (Chander, 2020: pp. 777-778).

The mutual recognition model involves reciprocal acceptance of each party's regulatory framework as sufficient despite differences in specific rules (Nicolaïdis, 2020: pp. 115-116). This approach, seen in the EU-U.S. Privacy Shield (before its invalidation) and the EU-Japan mutual adequacy decision, focuses on regulatory outcomes rather than identical rules. It potentially offers greater reciprocity than

unilateral adequacy decisions but still requires substantial alignment on core principles and enforcement mechanisms. The implementation challenges are considerable, as illustrated by the European Court of Justice's invalidation of both the Safe Harbor and Privacy Shield frameworks for EU-U.S. data transfers (Court of Justice of the European Union, 2020).

The regulatory harmonisation model pursues convergence toward common standards, reducing or eliminating differences between national regulatory frameworks. This approach, seen in the OECD Privacy Guidelines and the APEC Privacy Framework, aims to establish shared principles while allowing flexibility in implementation (OECD, 2013; APEC, 2015). Harmonisation potentially offers the greatest facilitation of data flows by minimising regulatory differences, but it faces political resistance from jurisdictions with distinctive approaches or sovereignty concerns.

The accountability model focuses on holding data controllers responsible for ensuring that data remains appropriately protected regardless of location, through contractual mechanisms, corporate binding rules, or certification schemes (Kuner, 2009: p. 263). This approach, recognised in both the GDPR and various trade agreements, shifts responsibility from regulatory compatibility to organizational compliance measures. It potentially accommodates greater regulatory diversity while maintaining protection but raises questions about monitoring and enforcement across jurisdictions.

Each of these models offers potential pathways for facilitating cross-border data flows while preserving legitimate regulatory objectives. Rather than selecting a single approach, an effective framework for digital trade governance might incorporate elements from multiple models, applying different cooperation mechanisms depending on the context and the regulatory domains involved (Mitchell & Mishra, 2018: p. 1113).

### 6.2. Interoperability versus Standardization Approaches

The tension between interoperability and standardisation represents a central challenge in digital trade governance. Interoperability approaches focus on making diverse regulatory systems work together through mechanisms like mutual recognition, equivalence determinations, or accountability frameworks. Standardisation approaches, by contrast, seek convergence on common rules, principles, or technical standards (Streinz, 2021: p. 873).

Interoperability approaches offer several advantages in the context of data governance. They accommodate legitimate regulatory diversity, recognising that differences in legal systems, social values, and institutional contexts may justify different approaches to common problems. They preserve greater policy space for experimentation and context-specific solutions, potentially fostering regulatory innovation. They may also be more politically feasible than standardisation, given the significant sovereignty concerns associated with data governance (Chander & Lê, 2015: p. 713).

However, interoperability approaches also present substantial challenges. They typically involve complex institutional mechanisms for assessing and maintaining compatibility between different systems, generating administrative costs and potential uncertainty. They may struggle to address fundamental divergences in regulatory philosophy or enforcement capacity. They sometimes create opportunities for regulatory arbitrage, where businesses structure their operations to exploit differences between regimes (Casalini, González, & Nemoto, 2021: p. 21). Standardisation approaches offer complementary advantages. They reduce compliance costs for businesses by establishing uniform rules across jurisdictions. They potentially create a more level playing field by subjecting all market participants to identical requirements.

Yet standardisation approaches face their own limitations. They risk imposing inappropriate one-size-fits-all solutions that fail to account for legitimate contextual differences. They potentially privilege the approaches of dominant economies, which can more effectively advance their regulatory models in international negotiations. They may also stifle regulatory innovation by locking in particular approaches before their consequences are fully understood (UNCTAD, 2019: p. 131).

Given these trade-offs, an effective framework for digital trade governance likely requires both interoperability and standardization elements applied selectively to different aspects of data regulation. Common standards may be appropriate for technical issues with limited normative dimensions, while interoperability mechanisms may better address areas with significant value judgments or contextual considerations (Mitchell & Mishra, 2018: p. 1114). This selective approach could preserve the benefits of regulatory alignment while accommodating legitimate diversity where it matters most.

### 6.3. The Role of Technical Standards and Private Governance

Technical standards and private governance mechanisms play an increasingly important role in digital trade governance, complementing and sometimes substituting for traditional treaty rules. These mechanisms include international technical standards developed by bodies like the International Organisation for Standardisation (ISO), industry codes of conduct, corporate social responsibility initiatives, and multistakeholder governance frameworks (Mitchell & Mishra, 2018: p. 1114).

Technical standards contribute to digital trade governance in several ways. They establish common technical specifications that facilitate interoperability between different systems and services. They incorporate normative judgments about appropriate practices for data security, privacy protection, and other regulatory objectives. They provide reference points for regulatory compliance, with many legal frameworks explicitly incorporating or referencing technical standards. They potentially bridge regulatory differences by establishing common practices across jurisdictions with different formal rules (Streinz, 2019: p. 312).

Private governance initiatives similarly offer potential pathways for addressing

digital trade challenges. Industry codes of conduct can establish common expectations for responsible data practices, potentially going beyond minimum legal requirements. Certification mechanisms can provide assurance about compliance with particular standards or principles, reducing information asymmetries in the market. Corporate binding rules can establish consistent data protection across multinational operations spanning multiple jurisdictions (Kuner, 2010: p. 22).

These private and technical governance mechanisms offer several advantages in the digital context. They potentially respond more rapidly to technological developments than traditional treaty negotiations or legislative processes. They incorporate specialised expertise from technical communities and industry practitioners. They sometimes achieve greater global reach than legal instruments, particularly in jurisdictions with limited regulatory capacity. They can also potentially transcend political deadlocks that impede formal international agreements (Gasser, 2016: p. 65).

However, technical standards and private governance also present limitations and concerns. They raise questions about legitimacy and representation, as standard-setting processes may be dominated by particular stakeholders or interests. They potentially lack effective enforcement mechanisms, relying primarily on market incentives or reputational consequences. They sometimes exacerbate power asymmetries, as resource constraints may limit participation by developing countries or civil society groups. They also risk fragmenting governance across competing standards or frameworks (Wiener, 2009: p. 155).

An effective approach to digital trade governance should, therefore, incorporate technical standards and private governance while addressing these limitations. This might involve formal recognition of technical standards in trade agreements, coupled with procedural requirements for standard-setting processes. It could include mechanisms for broader participation in standard development, particularly from developing countries. It might establish relationships between private governance initiatives and public regulatory frameworks, leveraging their complementary strengths (Mitchell & Mishra, 2018: p. 1121).

### 6.4. Building Consensus between Developing and Developed Economies

The divide between developing and developed economies represents a fundamental challenge for digital trade governance. Developed economies, with established digital sectors and technological advantages, have typically advocated for liberal cross-border data flows with limited restrictions (Burri, 2021: pp. 28-30). Developing economies concerned about digital dependency and the distribution of benefits from digital trade have often sought to preserve greater policy space for domestic digital development strategies (Gurumurthy, Vasudevan, & Chami, 2017: pp. 3-4). Bridging this divide requires addressing both the substantive interests at stake and the procedural conditions for inclusive participation in governance.

Substantively, effective governance must account for the asymmetric impacts

of digital trade liberalisation. While reducing barriers to data flows potentially benefits all economies through efficiency gains and innovation, the distribution of these benefits depends on factors like digital infrastructure, human capital, market size, and governance capacity (UNCTAD, 2021: pp. 87-92). Without accompanying measures to address these structural factors, liberalization alone may exacerbate rather than reduce digital divides.

A balanced approach would recognise legitimate concerns about digital dependency while creating pathways for developing countries to participate effectively in digital markets. This might involve provisions for digital capacity building, technology transfer, and technical assistance integrated into trade agreements rather than treated as separate development issues (Burri, 2017b: p. 128). It could include special and differential treatment provisions tailored to the digital context, providing greater flexibility for developing countries with limited digital capacities. It might explicitly preserve policy space for legitimate digital development strategies while establishing disciplines against purely protectionist measures.

Procedurally, effective governance requires more inclusive participation in rule-making processes. Developing countries have been underrepresented in many digital governance forums, from technical standard-setting bodies to trade negotiations, limiting their influence over emerging rules with significant development implications (UNCTAD, 2021: p. 149). This underrepresentation reflects various factors, including resource constraints, technical capacity limitations, and power asymmetries in international institutions.

Addressing these procedural challenges requires reforms to both institutional structures and negotiating processes. This might involve dedicated support for developing country participation in digital governance forums, including funding for technical expertise and capacity building. It could include more transparent and accessible negotiating processes, with opportunities for meaningful input from diverse stakeholders. It might also entail greater use of inclusive governance models that explicitly incorporate development perspectives, such as the multistakeholder approach pioneered in internet governance (Ciuriak & Ptashkina, 2018: p. 22).

The success of any framework for digital trade governance ultimately depends on building genuine consensus between developing and developed economies, not merely imposing the preferences of dominant digital powers. This consensus must be based on mutual recognition of legitimate interests and concerns alongside a shared commitment to a digital economy that generates widely distributed benefits. While challenging to achieve, such consensus represents the only sustainable foundation for global digital trade governance.

### 6.5. Proposals for WTO Negotiations on E-Commerce

The ongoing WTO negotiations on e-commerce, conducted through the Joint Statement Initiative (JSI) launched at the 2017 Buenos Aires Ministerial Conference, represent the most significant current effort to develop multilateral rules for digital trade (WTO, 2019). These negotiations involve 86 WTO members ac-

counting for over 90% of global trade and address various aspects of e-commerce, including cross-border data flows, data localisation, privacy protection, and digital customs duties (WTO, 2021).

Several proposals have emerged from these negotiations, reflecting different perspectives on digital trade governance. Developed economies like the United States, Japan, and Singapore have generally advocated for provisions prohibiting restrictions on cross-border data flows and data localisation requirements, subject to exceptions for legitimate public policy objectives (Communication from Japan, 2019). The European Union has proposed a more qualified approach, emphasising the importance of data protection and proposing that data flow provisions be accompanied by enforceable commitments on privacy protection (Communication from the European Union, 2019). Developing countries have emphasized the need for policy space, capacity building, and bridging digital divides, with some expressing concerns about the implications of data flow liberalization for digital development (Communication from a Group of Developing Countries, 2019).

These divergent positions reflect not only different economic interests but also different conceptions of the relationship between trade liberalisation and regulatory autonomy in the digital sphere. The challenge for negotiators is to develop provisions that facilitate beneficial data flows while accommodating legitimate regulatory diversity and addressing development concerns. Several approaches might contribute to this objective.

First, negotiators could adopt a layered approach to data governance, with different rules applying to different categories of data based on their sensitivity and regulatory implications (Mitchell & Mishra, 2018: p. 1133). This might involve stronger disciplines for data with limited privacy or security implications, coupled with greater flexibility for more sensitive categories where regulatory concerns are most acute.

Second, negotiators could develop more sophisticated exception provisions tailored to the digital context. Rather than simply transplanting traditional exceptions from the GATT or GATS, these provisions could explicitly address the distinctive regulatory challenges posed by data flows, with guidance on their interpretation and application (Streinz, 2019: p. 327). This might include recognition of data protection as a legitimate objective in its own right, not merely as an aspect of privacy protection.

Third, negotiators could incorporate substantive provisions on capacity building, technical assistance, and digital infrastructure development integrated with the trade rules rather than treated as separate development issues (Burri, 2017b: p. 128). This approach would recognize that meaningful participation in digital trade requires not only market access but also the capacity to utilize that access effectively.

Fourth, negotiators could establish institutional mechanisms for ongoing dialogue and cooperation on digital regulatory issues beyond the initial agreement

(Gao, 2018: p. 319). These mechanisms could address emerging technologies and business models not contemplated during the negotiations, facilitate regulatory learning across jurisdictions, and provide forums for addressing tensions before they escalate into formal disputes.

The JSI negotiations face significant challenges, including questions about their relationship to the broader WTO framework and concerns about their inclusivity (Kelsey, 2018: p. 275). However, they also represent a promising opportunity to develop multilateral rules that could reduce fragmentation, enhance predictability, and facilitate beneficial digital trade while respecting legitimate regulatory objectives. The outcome of these negotiations will significantly shape the future landscape of digital trade governance.

## 7. Conclusion

### 7.1. Principal Findings and Implications for Policymakers

This examination of cross-border data flows within the international trade legal framework reveals several principal findings with significant implications for policymakers. First, the existing WTO agreements, negotiated in the pre-internet era, provide an inadequate foundation for governing digital trade in general and cross-border data flows in particular. The classification challenges, interpretative uncertainties, and conceptual limitations of these agreements create substantial legal ambiguity about the rules applicable to data flows, undermining predictability and potentially enabling disguised protectionism (Dayday, 2023: p. 33).

Second, regional trade agreements have emerged as important laboratories for developing new approaches to digital trade governance, with the CPTPP and RCEP representing contrasting models balancing liberalisation and regulatory autonomy. The CPTPP establishes stronger disciplines on data flow restrictions and localization requirements, with narrower exceptions, while the RCEP preserves greater regulatory flexibility through broader exceptions and self-judging security provisions (Streinz, 2021: pp. 3-4). These divergent approaches reflect legitimate differences in regulatory philosophy and priorities among the participating countries.

Third, the tension between trade liberalisation and legitimate regulatory objectives in the data sphere can be accommodated through appropriately designed exception provisions, but these must be calibrated to preserve both meaningful disciplines against protectionism and genuine policy space for privacy protection, security measures, and other legitimate objectives. The necessity test plays a crucial role in this balancing exercise, requiring that trade-restrictive measures be proportionate to their regulatory objectives and not more trade-restrictive than necessary (Korea-Beef, 2001: para 164).

Fourth, effective governance of cross-border data flows requires moving beyond binary conceptions of data localization versus free flow, recognizing instead the diverse regulatory interests at stake and the potential for innovative approaches that facilitate beneficial flows while addressing legitimate concerns. Models like accountability frameworks, mutual recognition arrangements, and common stand-

ards offer potential pathways for reconciling these competing objectives, though each presents its own implementation challenges (Mitchell & Mishra, 2018: pp. 1111-1115).

Fifth, the asymmetric impacts of digital trade liberalisation demand particular attention to development dimensions in any governance framework. Without accompanying measures to address digital divides in infrastructure, skills, and regulatory capacity, liberalization alone may exacerbate rather than reduce economic inequalities. Inclusive governance requires substantive provisions addressing these structural factors and procedural mechanisms, ensuring the meaningful participation of developing countries in rule-making processes (UNCTAD, 2021: p. 149).

These findings have profound implications for policymakers engaged in digital trade governance. At the multilateral level, they suggest that WTO reform efforts should focus not merely on extending existing disciplines to the digital realm but on developing new approaches that explicitly address the distinctive characteristics of data and digital services. The ongoing JSI negotiations on e-commerce offer an opportunity to pursue such innovation, though their success depends on striking an appropriate balance between liberalisation and regulatory autonomy (WTO, 2019).

At the regional and bilateral levels, policymakers should seek greater coherence among proliferating data provisions while accommodating legitimate regulatory diversity. This might involve developing model provisions or guidelines that provide a common framework while preserving flexibility for context-specific implementation. Convergence on basic principles and procedural requirements could reduce fragmentation while respecting different substantive approaches to data governance (Burri, 2021: p. 36).

At the domestic level, policymakers should design data regulations with international trade implications in mind, ensuring that measures are genuinely tailored to their objectives and not more trade-restrictive than necessary. This does not mean subordinating legitimate regulatory goals to trade interests, but rather pursuing these goals through measures designed to minimize unnecessary trade friction. Regulatory impact assessments should explicitly consider effects on cross-border data flows and explore less trade-restrictive alternatives where available (OECD, 2020: p. 25).

Collectively, these implications point toward a more nuanced approach to digital trade governance—one that recognizes the economic importance of cross-border data flows while acknowledging the legitimate diversity of regulatory approaches to data governance. The challenge for policymakers is to develop frameworks that facilitate beneficial data flows while preserving meaningful policy space for pursuing domestic regulatory objectives.

### 7.2. Future Challenges and Research Directions

The governance of cross-border data flows faces several emerging challenges that will shape its future development and require further research. Technological evo-

lution continues to transform the nature and scale of data flows, with developments like artificial intelligence, the Internet of Things, and distributed ledger technologies creating new governance challenges not contemplated in existing frameworks (UNCTAD, 2019: pp. 103-105). These technologies generate novel questions about liability, security, transparency, and jurisdiction that existing rules are ill-equipped to address.

Geopolitical tensions increasingly influence approaches to data governance, with competing visions of digital order emerging from major powers (Farrell & Newman, 2019: p. 46). The United States has generally advocated a liberal approach emphasising free flows with limited restrictions. The European Union has developed a third approach emphasizing regulatory power to advance fundamental rights and societal values. These competing visions complicate efforts to develop coherent global governance frameworks.

Digital development concerns have gained prominence as developing countries recognize both the opportunities and risks of integration into global data flows (UNCTAD, 2021: pp. 87-92). Questions about the distribution of benefits from digital trade, the impacts of network effects and first-mover advantages, and the appropriate development strategies for digital economies have become central to governance debates. These concerns demand research on the relationship between data governance approaches and development outcomes, moving beyond abstract efficiency arguments to examine distributional implications.

The regulatory capacity challenges affecting governance implementation across jurisdictions deserve particular research attention, especially for developing countries. Many of these nations face a triple challenge: insufficient technical expertise to understand complex data flows, limited institutional resources to develop and enforce regulations, and inadequate digital infrastructure to participate effectively in global data economies (UNCTAD, 2021: pp. 125-127).

Future research should explore several promising pathways to address these capacity gaps. First, innovative institutional models could be developed that are specifically calibrated to the resource constraints of developing economies—perhaps emphasizing regional regulatory cooperation to pool limited expertise and resources. For example, the African Union's Convention on Cyber Security and Personal Data Protection offers a template for regional approaches that could be adapted to data flow governance (African Union, 2014).

Second, graduated implementation frameworks deserve exploration, allowing developing countries to phase in regulatory requirements as their capacity develops. Such frameworks might include extended transition periods for implementing certain obligations, simplified initial compliance requirements, and benchmarking systems to measure the progressive realization of regulatory goals. The TRIPs Agreement's differentiated implementation periods for developing and least-developed countries provide a useful precedent that could be adapted to digital governance contexts.

Third, targeted capacity-building programs need to be integrated directly into

trade agreements rather than treated as separate development assistance. These could include technical training programs, regulatory fellowship exchanges, and knowledge transfer mechanisms specifically focused on data governance. The WTO's Aid for Trade initiative could be expanded to include a dedicated digital governance component with measurable outcomes and sustainable funding mechanisms.

Fourth, appropriate technology solutions should be researched to amplify limited regulatory resources in developing countries. Regulatory technology ("RegTech") approaches using automation, AI-assisted compliance monitoring, and standardized reporting frameworks could help bridge capacity gaps while reducing implementation costs. Such technological approaches must be designed with developing country contexts in mind, emphasizing accessibility, low resource requirements, and integration with existing systems.

Crucially, this research agenda must engage developing country stakeholders as active participants rather than passive recipients of governance models designed elsewhere. This participatory approach would help ensure that capacity-building efforts address actual needs and constraints rather than imposing inappropriate governance frameworks developed for advanced digital economies.

Furthermore, addressing these challenges requires interdisciplinary research that transcends traditional disciplinary boundaries. Legal analysis must engage with a technical understanding of data flows and their economic impacts. Economic analysis must incorporate insights from political science about power dynamics and institutional constraints. Normative considerations from ethics and political philosophy must inform assessments of different governance approaches and their implications for values like privacy, autonomy, and distributive justice (Cohen, 2017: pp. 184-186).

Several specific research directions merit particular attention. Empirical analysis of the economic impacts of different data governance approaches could provide evidence to inform the necessity and proportionality assessments central to exception provisions. Comparative institutional analysis of different regulatory cooperation models could identify the conditions under which each approach is most effective. Case studies of regulatory innovation in specific sectors or jurisdictions could generate insights about promising governance practices that might be adapted to other contexts (Mitchell & Mishra, 2018: p. 1135).

More fundamentally, research should explore the conceptual foundations of data governance, examining how principles developed for physical trade might be adapted to the distinctive characteristics of data flows. This conceptual work requires engaging with questions about the nature of digital sovereignty, the appropriate balance between harmonization and regulatory autonomy, and the relationship between trade rules and other governance regimes addressing data (Streinz, 2021: p. 875). Only by addressing these foundational questions can we develop governance frameworks capable of addressing current and future challenges in cross-border data flows.

### 7.3. Final Reflections on Balancing Trade Liberalization and Regulatory Autonomy

The governance of cross-border data flows exemplifies a central tension in contemporary international economic law: the challenge of reconciling the benefits of economic integration with the legitimate exercise of regulatory sovereignty. This tension is not unique to the digital realm, but it manifests in distinctive ways given the intangible, replicable, and pervasive nature of data flows in the modern economy (Burri, 2021: p. 11).

The analysis in this paper suggests that effective governance requires moving beyond simplistic dichotomies between free flows and data sovereignty. Neither unrestricted data flows nor unlimited regulatory discretion provides a sustainable foundation for digital trade governance. Instead, we need frameworks that facilitate beneficial flows while preserving meaningful policy space for legitimate regulatory objectives—frameworks that recognise both the economic value of data integration and the social, political, and cultural values expressed through distinctive regulatory approaches (Yakovleva & Irion, 2020: p. 220).

Such balanced governance is challenging but not impossible. The exception provisions in trade agreements offer one mechanism for reconciling trade and regulatory objectives, though their effectiveness depends on interpretation and application. Regulatory cooperation models provide another pathway, focusing on making diverse systems work together rather than imposing uniformity. Technical standards and private governance mechanisms offer complementary approaches that can address specific aspects of data governance while leaving broader value judgments to public authorities (Mitchell & Mishra, 2018: p. 1121).

Ultimately, the governance of cross-border data flows is not merely a technical challenge but a profoundly political one, involving choices about the relative priority of different values and interests. These choices cannot be resolved through legal analysis alone but require inclusive dialogue among stakeholders with diverse perspectives. The goal should not be eliminating the tension between trade liberalisation and regulatory autonomy—a tension that reflects genuine pluralism in values and priorities—but rather managing this tension in a manner that preserves the benefits of both dimensions (Dayday, 2023: p. 81).

The evolution of international trade law in response to the digital transformation remains incomplete, with significant questions unresolved and new challenges continually emerging. However, the exploration in this article suggests potential pathways toward governance frameworks that can navigate the competing imperatives of the digital age. By acknowledging legitimate regulatory diversity while establishing common principles and disciplines, such frameworks could facilitate beneficial data flows while respecting the distinctive social, cultural, and political contexts in which these flows operate. Developing these balanced frameworks represents one of the most significant challenges and opportunities for international economic law in the twenty-first century.

## Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

## References

Aaronson, S. A. (2016). At the Intersection of Cross-Border Information Flows and Human Rights: TPP as a Case Study. *Georgetown Journal of International Affairs, 14,* 15-23.

Aaronson, S. A. (2019). What Are We Talking about When We Talk about Digital Protectionism? *World Trade Review, 18,* 541-577. https://doi.org/10.1017/s1474745618000198

African Union (2014). *African Union Convention on Cyber Security and Personal Data Protection*. https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

APEC (2015). *APEC Privacy Framework*. Asia-Pacific Economic Cooperation.

Bhagwati, J. (1995). *US Trade Policy: The Infatuation with FTAs*. Columbia University Department of Economics Discussion Paper Series No. 726.

Burri, M. (2017a). The Regulation of Data Flows through Trade Agreements. *Georgetown Journal of International Law, 48,* 407-448.

Burri, M. (2017b). The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation. *UC Davis Law Review, 51,* 65-132.

Burri, M. (2021). Data Flows and Global Trade Law. In M. Burri (Ed.), *Big Data and Global Trade Law* (pp. 11-41). Cambridge University Press. https://doi.org/10.1017/9781108919234.003

Burri, M., Polanco, R., Burri, S., & Lamin, M. (2022). *Trade Agreements Provisions on Electronic-Commerce and Data*. University of Lucerne. https://www.unilu.ch/en/faculties/faculty-of-law/professorships/burri-mira/research/taped/

Casalini, F., & González, J.L. (2019). *Trade and Cross-Border Data Flows*. OECD Trade Policy Papers No. 220, OECD Publishing.

Casalini, F., López González, J., & Nemoto, T. (2021). *Mapping Commonalities in Regulatory Approaches to Cross-Border Data Transfers*. OECD Trade Policy Papers No. 248, OECD Publishing.

Chander, A. (2020). Is Data Localization a Solution for Schrems II? *Journal of International Economic Law, 23,* 771-784. https://doi.org/10.1093/jiel/jgaa024

Chander, A., & Lê, U.P. (2015). Data Nationalism. *Emory Law Journal, 64,* 677-739.

Ciuriak, D., & Ptashkina, M. (2018). *The Digital Transformation and the Transformation of International Trade*. RTA Exchange Issue Paper, International Centre for Trade and Sustainable Development.

Cohen, J. E. (2017). Law for the Platform Economy. *UC Davis Law Review, 51,* 133-204.

Communication from a Group of Developing Countries (2019). *Development Aspects of Electronic Commerce and the Digital Economy*. INF/ECOM/12, World Trade Organization.

Communication from Japan (2019). *Joint Statement Initiative on Electronic Commerce*. INF/ECOM/4, World Trade Organization.

Communication from the European Union (2019). *Joint Statement Initiative on Electronic Commerce*. INF/ECOM/5, World Trade Organization.

Court of Justice of the European Union (2020). *Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*. ECLI:EU:C:2020:559. https://curia.europa.eu/juris/liste.jsf?num=C-311/18

CPTPP (2018). *Comprehensive and Progressive Agreement for Trans-Pacific Partnership*. https://www.dfat.gov.au/trade/agreements/in-force/cptpp/official-documents

Dai, Y. (2022). *Cross-Border Data Transfers Regulations in the Context of International Trade Law: A PRC Perspective*. Springer.

Dayday, C. M. G. T. (2023). Cross-Border Data Flows and Data Regulation under International Trade Law. *Philippine Law Journal, 96,* 33-81.

Drahos, P. (2002). Developing Countries and International Intellectual Property Standard-setting. *The Journal of World Intellectual Property, 5,* 765-789. https://doi.org/10.1111/j.1747-1796.2002.tb00181.x

Farrell, H., & Newman, A. L. (2019). Weaponized Interdependence: How Global Economic Networks Shape State Coercion. *International Security, 44,* 42-79. https://doi.org/10.1162/isec_a_00351

Ferracane, M. (2017). *Restrictions on Cross-Border Data Flows: A Taxonomy*. ECIPE Working Paper No. 1/2017, European Centre for International Political Economy. https://doi.org/10.2139/ssrn.3089956

Gao, H. (2018). Digital or Trade? The Contrasting Approaches of China and US to Digital Trade. *Journal of International Economic Law, 21,* 297-321. https://doi.org/10.1093/jiel/jgy015

Gasser, U. (2016). Recoding Privacy Law: Reflections on the Future Relationship among Law, Technology, and Privacy. *Harvard Law Review Forum, 130,* 61-70.

GATS (1995). *General Agreement on Trade in Services, 15 April 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183, 33 I.L.M. 1167*.

GATT (1994). *General Agreement on Tariffs and Trade 1994, 15 April 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1A, 1867 U.N.T.S. 187, 33 I.L.M. 1153*.

GDPR (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data. *Official Journal of the European Union, 119,* 1.

Gervais, D. (2016). *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future*. OECD Digital Economy Papers No. 187, OECD Publishing.

Greenleaf, G. (2021). *Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance* (pp. 1-5). Privacy Laws & Business International Report 169. https://doi.org/10.2139/ssrn.3836348

Gurumurthy, A., Vasudevan, A., & Chami, N. (2017). *The Grand Myth of Cross-Border Data Flows in Trade Deals*. IT for Change. https://itforchange.net/grand-myth-of-cross-border-data-flows-trade-deals

International Covenant on Civil and Political Rights (1966). Adopted 16 December 1966, Entered into force 23 March 1976, 999 UNTS 171.

International Organization for Standardization (2016). *How the Internet of Things Will Change Our Lives*. ISO Focus. https://www.iso.org/news/2016/09/Ref2112.html

Kelsey, J. (2018). How a TPP-Style E-Commerce Outcome in the WTO Would Endanger the Development Dimension of the GATS Acquis (and Potentially the WTO). *Journal of*

*International Economic Law, 21,* 273-295. https://doi.org/10.1093/jiel/jgy024

Kuner, C. (2009). Developing an Adequate Legal Framework for International Data Transfers. In S. Gutwirth, *et al.* (Eds.), *Reinventing Data Protection?* (pp. 263-273). Springer. https://doi.org/10.1007/978-1-4020-9498-9_16

Kuner, C. (2010). *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future*. OECD Digital Economy Papers No. 187, OECD Publishing. https://doi.org/10.2139/ssrn.1689483

Lateef, M. A., & Akinsulore, A. O. (2021). COVID-19: Implications for Corporate Governance and Corporate Social Responsibility (CSR) in Africa. *Beijing Law Review, 12,* 139-160. https://doi.org/10.4236/blr.2021.121008

Lemley, M. A. (1998). The Law and Economics of Internet Norms. *Chicago-Kent Law Review, 73,* 1257-1294.

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

Marrakesh Agreement Establishing the World Trade Organization (1994). Adopted 15 April 1994, Entered into Force 1 January 1995, 1867 UNTS 154.

Meltzer, J. P. (2014). The Internet, Cross-Border Data Flows and International Trade. *Asia & the Pacific Policy Studies, 2,* 90-102. https://doi.org/10.1002/app5.60

Mitchell, A. D., & Hepburn, J. (2018). WTO and Digital Trade. In T. Cottier, & M. Oesch (Eds.), *Handbook on the WTO and Technical Barriers to Trade* (pp. 196-221). Cambridge University Press.

Mitchell, A. D., & Mishra, N. (2018). Data at the Docks: Modernizing International Trade Law for the Digital Economy. *Vanderbilt Journal of Entertainment & Technology Law, 20,* 1073-1134.

Mitchell, A. D., & Mishra, N. (2021). WTO Law and Cross-Border Data Flows: An Unfinished Agenda. In M. Burri (Ed.), *Big Data and Global Trade Law* (pp. 83-112). Cambridge University Press. https://doi.org/10.1017/9781108919234.006

Nicolaïdis, K. (2020). Mutual Recognition: Promise and Denial, from Sapiens to Brexit. *Oxford Review of Economic Policy, 124,* 114-135.

OECD (2013). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. OECD Publishing.

OECD (2019). *Trade and Cross-Border Data Flows. OECD Trade Policy Brief*. OECD Publishing.

OECD (2020). *Regulatory Impact Assessment. OECD Best Practice Principles for Regulatory Policy*. OECD Publishing.

RCEP (2020). *Regional Comprehensive Economic Partnership Agreement, Signed 15 November 2020, Entered into Force 1 January 2022*. https://rcepsec.org/legal-text/

Streinz, T. (2019). Digital Megaregulation Uncontested? TPP's Model for the Global Digital Economy. In B. Kingsbury, *et al.* (Eds.), *Megaregulation Contested: Global Economic Ordering after TPP* (pp. 312-342). Oxford University Press. https://doi.org/10.1093/oso/9780198825296.003.0014

Streinz, T. (2021). RCEP's Contribution to Global Data Governance. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3826217

Trachtman, J. P. (1999). The Domain of WTO Dispute Resolution. *Harvard International Law Journal, 40,* 333-377.

UNCTAD (2019). *Digital Economy Report 2019: Value Creation and Capture: Implications for Developing Countries*. United Nations.

UNCTAD (2021). *Digital Economy Report 2021: Cross-Border Data Flows and Development: For Whom the Data Flow*. United Nations.

Universal Declaration of Human Rights (1948). Adopted 10 December 1948, UNGA Res 217 A(III).

Wang, W. (2020). Securing Cyberspace: China's National Cybersecurity Strategy and Legislation. In E. Bertino, P. Samarati, & J. Zhou (Eds.), *Cloud Computing and Security* (pp. 119-138). Springer.

Wiener, J. B. (2009). The Global Internet Governance Landscape I: Norms, Standards and Institutions. In L. A. Bygrave, & J. Bing (Eds.), *Internet Governance: Infrastructure and Institutions* (pp. 155-192). Oxford University Press.

World Trade Organization (2001). *Korea—Measures Affecting Imports of Fresh, Chilled and Frozen Beef*. Appellate Body Report, WT/DS161/AB/R, WT/DS169/AB/R.

World Trade Organization (2005). *United States—Measures Affecting the Cross-Border Supply of Gambling and Betting Services*. Appellate Body Report, WT/DS285/AB/R.

World Trade Organization (2010). *China—Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*. Appellate Body Report, WT/DS363/AB/R.

World Trade Organization (2019). *Russia—Measures Concerning Traffic in Transit*. World Trade Organization, WT/DS512/R.

WTO (1991). *Services Sectoral Classification List*. MTN.GNS/W/120, World Trade Organization.

WTO (2019). *Joint Statement on Electronic Commerce*. WT/L/1056, World Trade Organization.

WTO (2020). *World Trade Report 2020: Government Policies to Promote Innovation in the Digital Age*. World Trade Organization.

WTO (2021). *E-Commerce Negotiations: Members Finalize "Clean Text" on Unsolicited Commercial Messages*. World Trade Organization. https://www.wto.org/english/news_e/news21_e/ecom_05feb21_e.htm

WTO Ministerial Conference (1998). *Declaration on Global Electronic Commerce*. WT/MIN(98)/DEC/2. World Trade Organization.

Wu, T. (2006). The World Trade Law of Censorship and Internet Filtering. *Chicago Journal of International Law, 7,* 263-287.

Yakovleva, S., & Irion, K. (2016). The Best of Both Worlds? Free Trade in Services and EU Law on Privacy and Data Protection. *European Data Protection Law Review, 2,* 191-208. https://doi.org/10.21552/edpl/2016/2/9

Yakovleva, S., & Irion, K. (2020). Pitching Trade against Privacy: Reconciling EU Governance of Personal Data Flows with External Trade. *International Data Privacy Law, 10,* 201-221. https://doi.org/10.1093/idpl/ipaa003