BUILDING BLOCKS OF DIGITAL TRADE REGULATION SERIES
No. 4

Data and Digital Trade Law

Balancing rules, policy space, and development

IISD REPORT

Marilia Maciel

IISD
International Institute for Sustainable Development

April 2026

International Institute for Sustainable Development

The International Institute for Sustainable Development (IISD) is a globally recognized think tank with 3 decades of experience working to solve the world's most pressing sustainable development challenges. We combine deep expertise in a wide range of issues with a collaborative approach to research, policy advice, and hands-on support to ensure these solutions are brought to life. Headquartered in Winnipeg, Manitoba, we are a diverse team of over 300 professionals working from offices in Canada, Switzerland, and other locations around the world.

IISD's headquarters in Winnipeg are situated on Treaty 1 Territory—the ancestral lands of the Anishinaabe (Ojibwe), Ininiw (Cree), Anisininew (Ojibwe Cree), Dene, and Dakota Nations, and the homeland of the Red River Métis Nation.

IISD is a registered charitable organization in Canada and has 501(c)(3) status in the United States. IISD receives core operating support from the Province of Manitoba and project funding from governments inside and outside Canada, United Nations agencies, foundations, the private sector, and individuals.

Head Office

111 Lombard Avenue, Suite 325
Winnipeg, Manitoba
Canada R3B 0T4

iisd.org

Data and Digital Trade Law: Balancing rules, policy space, and development

April 2026

Written by Marilia Maciel (Director of Digital Trade and Economic Security, Diplo)

Photo:

Acknowledgements

The author would like to thank Arindrajit Basu, Henry Gao, Rashid S. Kaukab, Neha Mishra, Lucas da Silva Tasquetto, and Alice Tipping for their review and comments on the first draft of this note.

This report was produced with the support of the Swedish International Development Cooperation Agency (Sida).

Sweden Sverige

Sida

Table of Contents

List of Figures

List of Boxes

Abbreviations and Acronyms

AfCFTA	African Continental Free Trade Area
AI	artificial intelligence
CPTPP	Comprehensive and Progressive Agreement for Trans-Pacific Partnership
DEA	digital economy agreement
DEPA	Digital Economy Partnership Agreement
DTP	Digital Trade Protocol
EU	European Union
FDI	foreign direct investment
FRAND	Fair, Reasonable, and Non-Discriminatory
FTA	free trade agreement
GATS	General Agreement on Trade in Services
GATT	General Agreement on Tariffs and Trade
ICT	information and communications technology
ITA	Information Technology Agreement
LDC	least developed countries
MSME	micro small, and medium-sized enterprises
OECD	Organisation for Economic Co-operation and Development
OGD	open government data
PTA	preferential trade agreements
RCEP	Regional Comprehensive Economic Partnership
TAPED	Trade Agreement Provisions on Electronic Commerce and Data
UNCTAD	UN Trade and Development
WTO	World Trade Organization

1.0 Introduction

Data flows are essential for interpersonal communication and for the exercise of individual and collective rights. They also constitute the fabric of economic globalization, enabling the movement of goods, services, and capital: instantaneous financial settlements, real-time supply chain management, and the cross-border delivery of services depend on the ability to transfer data across jurisdictions. Data has become key for innovation and competitiveness, and it is also at the heart of geopolitical competition over artificial intelligence (AI) leadership.

The regulatory landscape has evolved rapidly in response to this multifaceted scenario. Across both developed and developing economies, governments are enacting domestic data governance measures to pursue a range of policy objectives related to trust and sovereignty concerns and to economic considerations. To pursue these objectives, governments often deploy regulatory instruments that affect the movement of data. This paper focuses on this critical juncture, where domestic policy meets international trade.

Two data governance measures particularly express the tensions at this interface: limitations on cross-border data transfers and data localization requirements. The paper unpacks their underlying justifications, characteristics, and scope. It argues that the physical location of infrastructure does not necessarily translate into domestic value creation or home-grown digital industrialization, if it is not accompanied by measures to reshape the underlying distribution of value in digital markets, by holistic data governance, and competition policy, for example.

The international trade law framework is responding to the domestic regulatory uptake in this area, though primarily outside the World Trade Organization (WTO). A growing number of preferential trade agreements (PTAs) and dedicated digital economy agreements (DEAs) incorporate data-related provisions. The way in which they address cross-border data flows varies significantly: while some aim to limit countries' abilities to restrict cross-border flows, others aim to support the creation of regulated pathways for safe and trustworthy data sharing, establish common expectations for data openness and interoperability, and foster collaborative frameworks to unlock the economic and social value of data. Some modern digital trade agreements also encompass "new data economy issues," such as AI, financial technology (fintech), and digital identities, for example, pointing to a growing interface between digital trade law and the broader realm of digital governance.

The rapid development of this legal architecture occurs amid inequality and mounting geopolitical tension. A growing consensus warns that the wealth generated by the digital economy is becoming increasingly concentrated in a handful of countries and corporations. This economic divergence is compounded by the simultaneous fragmentation of both value chains and political ideologies, putting pressure on developing countries to position themselves along the fault lines. This paper identifies six interlinked domestic and international challenges faced by developing countries and least developed countries (LDCs) in their quest for equitable participation and long-term digital development, and presents some policy options.

The paper has six substantive sections. Section 2 establishes the foundational role of data in the digital economy and society, examining its unique characteristics, its centrality to economic activity and AI, and its place in geopolitical competition. Section 3 reviews the primary domestic policy objectives driving data regulations and their potential implications for cross-border trade. Section 4 details the key regulatory mechanisms—limitations on cross-border data transfers and data localization—that directly impact international data flows, analyzing the spectrum of approaches that countries may take at the domestic level. Section 5 analyzes the existing and emerging rules governing data within international trade law, from the WTO framework to innovative provisions in modern PTAs and DEAs, with particular attention to provisions on cross-border data transfers and data localization, personal data protection, open government data, and data innovation. By setting rules for how data must be handled, these broader obligations influence the feasibility, incentives, cost, and structure of international data flows. Section 6 examines the development considerations arising from the current landscape, including asymmetrical value capture, the policy space-capacity dilemma, and the implications of the current geoeconomic turn. Section 8 presents a range of policy considerations for navigating the complex interplay between data governance, trade law, and national objectives, emphasizing the importance of context-specific strategies, regional cooperation, and the link between legal commitments and implementation support.

2.0 The Foundational Role of Data in Digital Trade and Society

Data has become a buzzword, but the expression is often not defined. Etymologically, data is the plural of the Latin word "datum," which means "that which is given." Modern definitions build on this, with the Merriam-Webster Dictionary (2025) defining it as factual information, such as measurements or statistics, used as a basis for reasoning, discussion, or calculation. While this broad definition encompasses information in any form—from paper-based charts to the sound waves of a human voice—the digital economy is specifically concerned with digital data, or, in other words, with data represented in a discrete, binary format (using "0's" and "1's") that can be processed by computers.

The large-scale creation of digital data was enabled by digitization, the technical process of converting analog information into a digital format. This process accelerated dramatically: in 1995, only about 25% of global information was stored in digital format, a figure that rose to 94% by 2007 (Mayer-Schönberger & Cukier, 2013). The volume of data is growing rapidly and is expected to reach 182 zettabytes in 2025 (Statista, 2025). For perspective, this is equivalent to approximately 58 trillion hours of high-definition video, enough for every person on Earth to watch without interruption for approximately 20 years. With the rise of AI, more data is projected to be generated between 2025 and 2027 than in all prior human history (Yap, 2024).

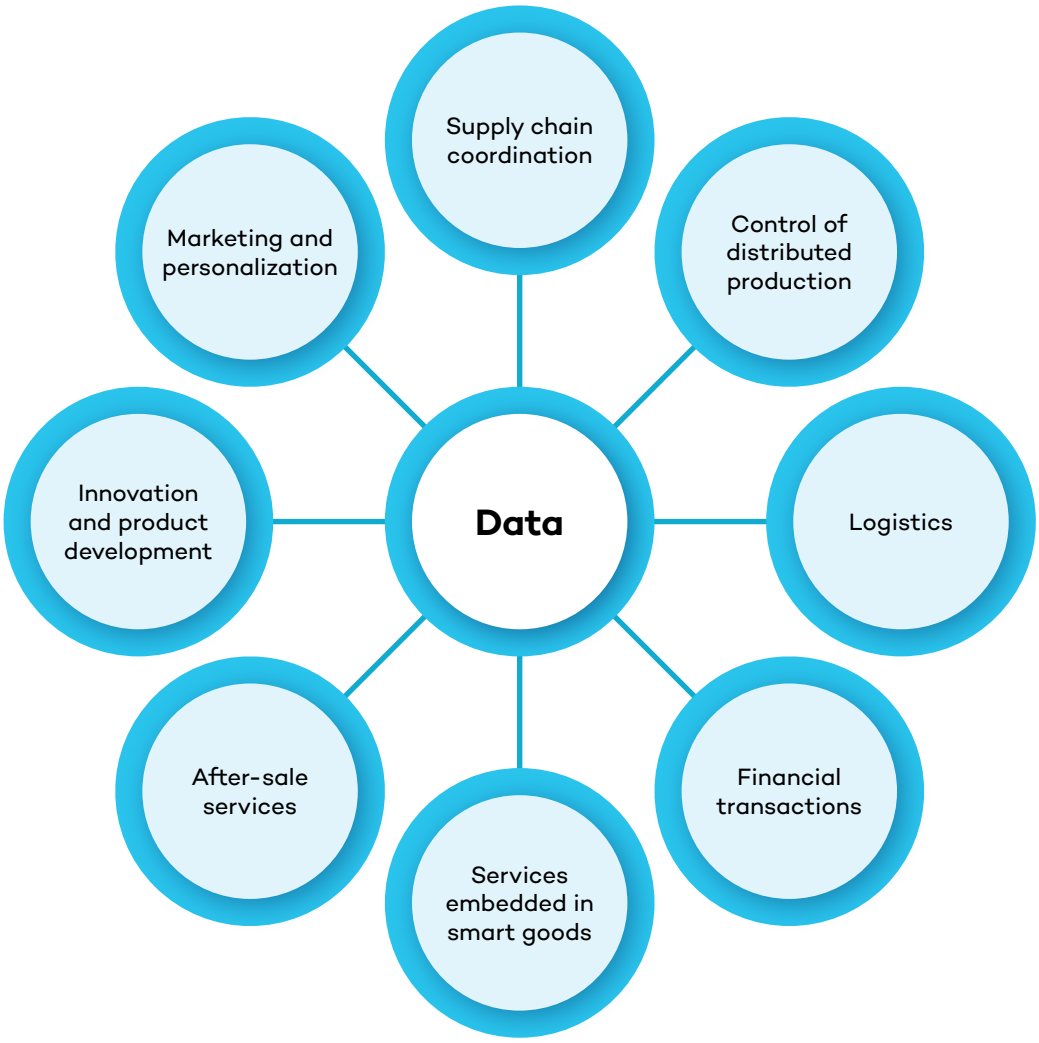
This mass digitization engendered digitalization: the transformation of social and economic activities through the intensive use of digital data and technologies (Organisation for Economic Co-operation and Development [OECD], 2019a). For instance, the digitalization of governmental services produced "e-government," while the digitalization of trade enabled "e-commerce." Society-scale digital transformation was made possible by two technological advancements. On the one hand, there was an exponential increase in the processing capacity of computers, powered by the evolution of semiconductors, allowing data to be analyzed faster than ever before. On the other hand, advancements in networking enabled the development of the global Internet. Together, they created the conditions for cross-border data flows.

Data flows are a multifunctional conduit. They enable interpersonal communication, from social interactions to the expression of political speech. Simultaneously, these flows constitute the essential fabric of economic globalization. They enable the coordination of complex supply chains and distributed production, facilitate access to foreign markets and global payments. In essence, data flows are the critical enabler for the cross-border movements of goods, services, and capital: financial transactions rely on instant cross-border data exchange; logistics and supply chains use real-time tracking and analytics; and many services that were once considered non-tradable, such as education, have become digitally deliverable because data can flow across jurisdictions (International Monetary Fund et al., 2023).

The critical role of data is evident in the servicification of trade. Servicification refers not only to products that were previously attached to a physical device (such as CDs in the case of music, now increasingly streamed as bits and bytes over the Internet), but also to the

embedding of data-intensive services into manufactured "smart" goods (Burri & Chander, 2023), such as the apps that accompany fitness equipment. It also refers to a broader process of corporate transformation, showing an increasing dependence on services by manufacturing firms (Willemyns, 2021). In this context, data plays a key role. For example, General Electric has shifted its business model by putting data analytics at its core (Henke et al., 2016), while Ford started to define itself as a "mobility company" and not just a car manufacturer (Kaas & Fleming, 2014). These changes will make cross-border data flows a cornerstone of global trade in the years to come.

Figure 1. The centrality of data in the global economy

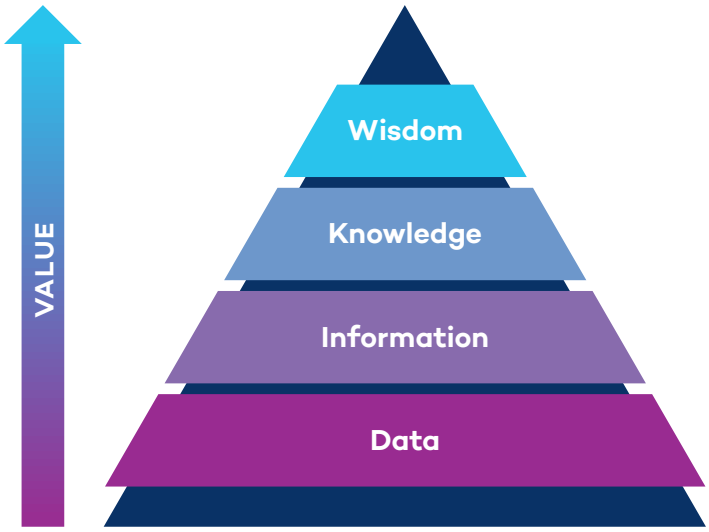


Source: Author.

While the ability to move data across borders is important, its true economic value is realized only when it is transformed into actionable knowledge (Ciuriak, 2022a; Guglya & Maciel, 2020). The data-information-knowledge-wisdom (DIKW) model (see Figure 2) illustrates this progression: data is contextualized into information, which is then interpreted to produce knowledge, and ultimately informs strategic wisdom (Ackoff, 1989; Rowley, 2007). Data provides the foundational building blocks for this entire structure.

The pursuit of wisdom—the highest stage of the DIKW hierarchy, which relies on accumulated knowledge to guide strategic action—explains the significant value placed on data-driven decision making across both public and private sectors. However, attempts to extract and appropriate knowledge have also triggered a race to harvest data on an unprecedented scale. As data has become an integral byproduct of daily life, this race leads to a de facto appropriation of social activity, where human experience is systematically mined for profit (Mejias & Couldry, 2019; Rikap, 2022).

Figure 2. The DIKW model



Source: Adapted from Guglya and Maciel, 2020.

Data has become a key object of global exchange, sparking debates on how to structure formal and informal markets for its trade. Leading this shift, China has formally designated data as a fundamental "factor of production," alongside traditional inputs like land and labour (Chen, 2022). In parallel, international bodies like the United Nations Commission on International Trade Law are working to develop harmonized contract rules to facilitate cross-border data transactions (United Nations General Assembly, 2025).

Data, processing power, and algorithms are the three essential inputs to AI. Although AI depends on several aspects of trade policy—i.e., trade in goods for access to specialized hardware, and trade in services for access to processing capacity and to specialized skills—access to data is paramount (Ferencz et al., 2022). As Ciuriak (2022a, p. 2) argues, the emergence of an "industrialisation of innovation through machine learning" is pushing countries toward preemptive strategies aimed at securing first-mover advantages or avoiding the risks of technological lag.

This dynamic not only justifies state-led digital industrial strategies but also positions data at the heart of geopolitical competition over AI leadership (Ciuriak, 2022a). As a consequence, data is increasingly reframed as a source of national power, essential for innovation and competitiveness in strategic sectors (Zhang & Gao, 2025). This shift, however, raises concerns about the data economy's unequal distribution of benefits and the potential emergence of a

new data colonialism, in which power imbalances are extended and entrenched through data control (Couldry & Mejias, 2018).

Against this backdrop, states are increasingly turning to the notion of data sovereignty to justify regulatory interventions. While sovereignty offers a rhetorical rallying cry, its ambiguity often obscures underlying policy objectives (Basu, 2023; Belli et al., 2024). Data sovereignty may be invoked to address myriad goals, such as promoting information security, personal data protection, and the economic rights of communities over their data, as well as the ambition of harnessing data for national development. This conflation of disparate agendas under a single banner contributes to a growing politicization of cross-border data flows.

While often considered "a new form of capital for the 21st century knowledge economies" (OECD, 2019b, p. 60), data possesses unique characteristics that distinguish it when compared to traditional capital inputs, such as physical tools and machinery (Carrière-Swallow & Haksar, 2019). These characteristics are central to contemporary policy debates. First, data is non-rivalrous. Its use by one actor does not diminish its availability or value for others. Second, it generates compound value. Integrating disparate data sets creates novel insights exceeding the sum of their parts. Finally, data is non-depletable, as it can be reused infinitely without being consumed, creating a powerful incentive for open data policies.

In spite of these characteristics, which inherently encourage data sharing, including across borders, access to data and to its benefits is currently unequal and increasingly concentrated (UN Trade and Development [UNCTAD], 2021). This can be explained by several factors. First, the value of data is contingent on infrastructure and algorithms. The capacity to extract value from data is not distributed evenly. More than 50% of the world's hyperscale data centres are located in the United States and China (UNCTAD, 2021). Global spending on cloud infrastructure services rose 21% in 2025, but remained concentrated in the three cloud providers (AWS, Microsoft Azure, and Google Cloud), with their combined market share accounting for 65% of global cloud spending (Omdia, 2025). Several countries still lack the infrastructure necessary to extract value from data.

Secondly, data is often made excludable. While its fundamental nature is non-rivalrous, entities that control data can create artificial scarcity through legal, commercial, or technical barriers. Public sector bodies may withhold data to protect privacy, national security, or commercially sensitive information. In the private sector, firms routinely use intellectual property rights and contractual agreements to prevent competitors from accessing their data sets. Efforts to promote interoperability are also insufficient, since data control helps commercial actors create lock-in effects and market dominance. This ability to exclude, combined with data's network effects, has led to unprecedented accumulation of economic power in the hands of a few dominant digital firms. The result is a self-reinforcing cycle: companies with vast data sets can improve their services, attract more users, and gather even more data, entrenching their positions.

This dynamic, which lies at the core of many digital platform business models, raises concerns not only for competition and innovation but also for individual autonomy, human rights, and democracy (Aaronson, 2018; Whittaker, 2023). One key issue is that the data sets used to train machine learning systems may be unrepresentative, biased, or reflect historical inequalities,

potentially leading to algorithmic discrimination in areas such as credit, employment, and access to services (Casillas, 2022). At the same time, the large-scale collection of personal data enables detailed profiling and microtargeting, which can be used to influence and manipulate consumer behaviour (Paterson et al., 2021). This high degree of personalization may also contribute to social polarization, as platform algorithms are designed to prioritize content that maximizes user engagement, including sensationalist material and disinformation (Berger et al., 2024).

Data has emerged as a multifaceted resource that underpins economic activity, fuels AI development, shapes geopolitical competition, and is a subject of intense social contestation. While data is the lifeblood of digital trade, it also raises important social and political concerns. These competing dimensions increasingly shape national debates on data governance. They also spill over into international discussions on cross-border data transfers, where the benefits of data mobility must be weighed against societal risks, strategic interests, and public policy objectives.

3.0 Data Governance Measures Adopted at the Domestic Level and Potential Implications for Cross-Border Trade

Governments worldwide are increasingly enacting data governance measures. This regulatory drive can be exemplified by over 1,900 data-related policy developments introduced between 2020 and 2023 (Fritz & Giardini, 2023). While often designed for domestic objectives, these regulations create cross-border effects due to the interconnected nature of the digital economy. Consequently, interventions aimed at legitimate public policy goals may, intentionally or not, lead to a restriction of international data transfers. These restrictions are most commonly driven by the following policy objectives.

3.1 Privacy and Personal Data Protection

Privacy is a fundamental right, and it is also essential for digital trade, since data protection frameworks maintain the public trust that underpins business activity (Mishra, 2024). The protection of privacy has been a primary justification for restricting data flows, often by limiting or conditioning these flows in order to ensure data receives an "equivalent" level of protection in the destination jurisdiction (Casalini & López Gonzáles, 2019). Although there is a high-level consensus on principles of data protection at the international level, domestic frameworks and conditions for cross-border transfers differ along cultural and legal traditions, creating a fragmented landscape and increasing compliance costs that disproportionately impact micro small, and medium-sized enterprises (MSMEs).

3.2 Enforcement and Auditing

Governments may impose data flow restrictions to facilitate data access for regulatory oversight, audits, tax compliance, financial supervision, and law enforcement purposes, for example (Daskal, 2016). The underlying rationale is to ensure that domestic authorities can effectively exercise their jurisdiction and enforce local laws. In a globalized digital economy, data stored abroad can become subject to conflicting foreign legal regimes, creating barriers to access for legitimate purposes. Data flow restrictions aim to ensure that data remains accessible to national authorities aiming to apply national regulations and to maintain public order. In some cases, however, this rationale can also extend to more contentious goals, such as strengthening state control over information for censorship purposes (Akbari, 2026; Kugler, 2021). When targeted and sector-specific, such measures can strengthen public oversight. However, a careful balance is essential to avoid overly broad restrictions.

3.3 Cybersecurity Goals

States are increasingly enacting domestic cybersecurity regulations to protect critical infrastructure, businesses, and citizens. While legitimate, these measures create a complex interplay with international trade governance. The range of cybersecurity-based measures that

may have an impact on cross-border trade includes technology bans, licensing requirements, and restrictions on cross-border data flows (Mishra, 2025). These data flow restrictions may prohibit transfers to jurisdictions deemed "insecure" or make them conditional upon passing extensive security assessments and obtaining explicit regulatory approval.

3.4 National Security Concerns

In this case, measures restricting data flows seek to protect strategically sensitive data, such as military information, from foreign access. Their trade impact depends on whether measures are narrowly tailored to genuine security threats or applied broadly to commercial and user data under an expansive definition of national security (Steil & Harding, 2024). This distinction is further complicated by the growing interplay between national security and economic security. This is exemplified by changes in the United States' long-held support for binding commitments on data flows and against data localization. This policy change is driven not only by domestic considerations but also by the perceived need to counter strategic rivals, both in terms of national security and economic competitiveness (Sukumar & Basu, 2025).

3.5 Economic Security Concerns

Data governance is being driven by an interweaving of geopolitics and geoeconomic competition. In this context, governments are increasingly framing data governance as a tool for economic security (European Commission, 2025; Okano-Heijmans et al., 2023). Economic security can be understood as a state's ability to protect the competitiveness and resilience of its economy from geopolitical risks and strategic dependencies (Ghiretti, 2025). In the context of data governance, this rationale seeks to prevent industrial espionage and unauthorized access to sensitive data that could undermine competitiveness. The measures and tools used to achieve economic security goals include data localization, technology bans, export restrictions, investment screening (inbound and outbound), reinforced scrutiny over supply chains of hardware and software, reducing dependency on a single (or on a limited number) of suppliers of certain products and services, tighter control over mergers and acquisitions, and over the ownership of businesses possessing sensitive information or data[1] (Allison et al., 2025). As an example, the 2024 U.S. Executive Order on Sensitive Personal Data[2] seeks to prevent "countries of concern" from using U.S. data to erode U.S. technological competitiveness. Likewise, the EU Commission Communication on "Strengthening EU Economic Security" (European Commission, 2025) makes "preventing access to sensitive information and data" a cornerstone of the updated EU Economic Security Strategy (European Commission, 2023).

[1] The latter is illustrated by the U.S. law compelling the divestiture or ban of TikTok, a social media service owned by Chinese company ByteDance, for concerns over the transfer of U.S. citizens' data, among other reasons (Chander, 2022).

[2] United States of America. Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons. Department of Justice, 28 CFR Part 202 [Docket No. NSD 104], 1 August 2025.

3.6 Support for Industrial Policy Objectives

Data governance has become a strategic instrument for digital industrial policy (UNCTAD, 2024), with governments seeking to ensure that domestically generated data fuels local innovation and builds competitive digital sectors (Foster & Azmeh, 2020; Maciel, 2023). Some countries have made active use of data localization rules as a foundation for the development of a local ecosystem. Nevertheless, mandatory data localization has shown mixed results (Azmeh et al, 2021; Kugler, 2022). While legally mandated localization may foster the growth of domestic digital firms by increasing their revenue, it may also decrease overall consumer choice and service quality (Potluri et al., 2020). As an alternative to mandatory localization, some countries have opted for incentive-based approaches. A prime example is Brazil's REDATA Provisional Measure,[3] which uses tax incentives and access to renewable energy to attract major cloud providers (hyperscaler data centres). Nevertheless, this approach also reveals a tension between attracting foreign investment and building indigenous capacity, something particularly relevant for sectors in which data sovereignty over sensitive information is a strategic priority (Maciel et al., upcoming).

When discussing governmental data governance interventions, much attention is given to measures that may restrict data flows. Nevertheless, governments also actively implement policies to foster data access and cross-border data flows (OECD, 2022). Key interventions include open government data initiatives, which require public bodies to make non-sensitive data sets available for reuse, including for commercial purposes (OECD, 2019b). Similarly, mandatory data-sharing rules for private actors, often under FRAND (Fair, Reasonable, and Non-Discriminatory) terms, aim to stimulate competition and unlock economic value by facilitating data access across sectors. An example of the latter is found in the EU Data Act (European Union, 2023).

Critically, the distinction between restricting and enabling flows is not always clear-cut. Regulatory frameworks, such as the EU General Data Protection Regulation, which condition transfers on adequate data protection, are often characterized as barriers. However, they can also be understood as enablers of trustworthy data flows (OECD, 2022). By establishing clear rules and protections, they seek to create a balance between safeguarding key interests while maintaining data mobility.

The economic imperative for finding this balance is significant. As a joint OECD-WTO (2025) report highlights, frameworks that successfully combine cross-border flows with necessary safeguards can offset regulatory trade costs with the benefits of trust. The potential gains are substantial: a globally adopted balanced approach could boost global exports by 3.6% and global GDP by 1.77%, with lower-income economies seeing GDP growth of over 4% (OECD & WTO, 2025).

[3] Brazil, *Regime Especial de Tributação para Serviços de Datacenter- REDATA,* Medida Provisória n° 1318, de 2025.

4.0 Key Data Governance Mechanisms With an Impact on Cross-Border Trade: Limitations to cross-border data transfer and data localization

To pursue the diverse range of policy objectives discussed in Section 3, governments may deploy regulatory instruments that directly govern the movement of data. These mechanisms, particularly when they touch upon data crossing national borders, become the critical juncture where domestic policy meets international trade. In this section, we focus on the two most prominent data governance tools with explicit cross-border trade implications (Spiezia & Tscheke, 2020): limitations on cross-border data transfers and data localization requirements.

4.1 Limitations to Cross-Border Transfer of Data

Norms that establish limitations to cross-border transfer of data help to define whether, and in which circumstances, data can be transferred to actors located in another jurisdiction. These norms seek to establish regulated pathways for safe and trustworthy data flows. Depending on whether a country decides to introduce these limitations, and on their level of stringency, the following scenarios can be envisioned:

No Limitation to Cross-Border Transfers

In this case, countries do not impose restrictions on the cross-border movement of data. This often indicates the absence of certain domestic laws, such as privacy or security-related frameworks, for example. Although this scenario is permissive to cross-border flows, it may not be optimal from a socio-economic perspective. As the joint OECD-WTO (2025) report points out, the absence of regulation erodes trust and can negatively affect the willingness of firms in other countries to send data to these locations.

Transfers With Private Safeguards

This method grants the private sector discretion to manage data transfers using tools like standard contractual clauses and binding corporate rules. Companies must still adhere to domestic principles, and they face ex-post accountability if a breach or infringement occurs.

Transfers With Public Safeguards

This method requires authorization from a public authority ex-ante, before data can be transferred. This includes "adequacy" or "equivalence" decisions, which assess the legal framework of the country of destination.

Transfers Based on Ad Hoc Authorizations

The general approach is to prohibit transfers to other countries, allowing them only on a case-by-case basis, when there is an ad hoc authorization by public authorities.

Limitations on cross-border transfers may influence where data storage and processing will occur. The more stringent these limitations are, the more pressure there is to localize infrastructure in the territory of the country, introducing the regulation (Cory, 2021).

4.2 The Physical Location of Data Processing Infrastructure

The physical location of data storage and data processing infrastructure places this infrastructure (and the hosted data) under a country's jurisdictional authority (Schmitt & Vihul, 2017). This is important for governments for a variety of reasons, which can be grouped into two broad categories: trust and sovereignty concerns, and economic considerations. The first category includes several policy drivers discussed in Section 3, such as ensuring regulatory oversight, enabling law enforcement, protecting personal data, and promoting national security.

Beyond these regulatory and sovereignty-related motivations, data localization is also increasingly justified in economic terms, particularly with reference to its potential macroeconomic and sectoral effects. At the macroeconomic level, territorialization may affect a country's external accounts (Tozzi & Merki, 2025). In particular, where a country is a net importer of computing services, increased domestic provision of these services may reduce imports and contribute to an improvement in the services and financial accounts.

From a sectoral perspective, the development of data infrastructure within the national territory may generate economic spillovers, including demand for energy providers, construction firms, and support services, and may boost the growth of a domestic digital ecosystem by improving access to computing capacity (Singh et al., 2024). While data infrastructure is also often expected to foster domestic job creation, data centres employ relatively few high-skilled workers. Indirect employment (i.e., maintenance and connectivity) is strongly context dependent and tends to materialize only where a broader digital ecosystem already exists.

The physical location of data infrastructures can be influenced by offering rewards or introducing constraints (carrots or sticks). The first entails creating or strengthening local comparative advantages—i.e., the availability of energy, tax incentives, and the regulatory environment—that will make companies voluntarily decide to deploy infrastructure in a given territory. These types of measures are often placed under the scope of industrial policy.

The second way to influence the location of data infrastructure—which is often the focus of trade policy analysis—refers to "data localization" policies. In this case, data is stored or processed within a certain domestic territory due to an explicit legal requirement imposed by national authorities (López González et al., 2022).

Data localization measures will vary significantly, depending on the sector concerned, and also in relation to their underlying policy objectives (López González et al., 2022; OECD & WTO, 2025). Governmental approaches in relation to localization have engendered the following possible scenarios.

Local Storage Requirement, With No Subsequent Restriction on Data Flows

Countries require that a copy of certain data sets be kept within their territory, without prohibiting transfers to other countries if this baseline requirement is met. These measures are often applied to ensure that regulators do not encounter obstacles to the exercise of investigatory powers, oversight, or jurisdictional reach. They usually apply to specific data sets, such as tax and accounting records.

Local Storage and Processing Requirement, With Clearly Defined Transfer or Access Conditions

In this case, one out of two scenarios may take place:

1. The country allows data to be transferred abroad because the prerequisites established by law have been met. These prerequisites may entail mechanisms of ex-post accountability (i.e., the private sector has discretion to manage data transfers based on mechanisms such as standard contractual clauses), or mechanisms of ex-ante authorization, when a public authority must authorize the transfer of data according to pre-established rules (i.e., adequacy decisions).
2. If the prerequisites foreseen in the "regulated pathway" (Scenario 1) are not successfully met, data is kept within the country and cannot be transferred across borders. This second scenario becomes equivalent, in practice, to a local storage and processing requirement with a prohibition on transfer. This type of approach is often adopted in relation to personal data protection, for example.

Local Storage and Processing Requirements With Prohibitions on Transfer (or With Ad Hoc Permissions)

In this case, countries mandate local storage and processing of data by default, while also prohibiting transfers to other countries (or allowing transfer only on the basis of ad hoc authorizations). The mechanisms available in the "regulated pathway" (ex-post accountability or ex-ante authorizations) are deemed insufficient, often due to the highly sensitive nature of the data (i.e., health data, biometric data, and data that is relevant for national security).[4]

According to Giovane et al. (2023), the number of explicit data localization measures has been increasing, and the types of measures adopted have become more restrictive. Nearly half of the

[4] Examples of regulatory frameworks that establish local storage by default of personal, sensitive, important, or core data include: Russia's Federal Law No. 242-FZ (2014, amended) on Personal Data, China's "Cybersecurity Law and Data Security Law," as well as U.S. Executive Order on "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern."

existing measures have been introduced since 2015, reflecting the growing importance of data governance in national regulatory agendas.

Despite this expansion, localization alone cannot guarantee the fulfillment of key policy objectives such as trust and sovereignty concerns, and economic considerations. Jurisdiction is not determined solely by the physical location of data, but is also shaped by factors such as corporate nationality, contractual arrangements, and the extraterritorial reach of domestic laws. As a result, keeping data within national borders does not necessarily translate into effective regulatory control.

In this context, some governments have shifted their regulatory focus from where data is stored to whether domestic authorities can obtain timely access to it. Two prominent examples are the U.S. CLOUD Act and Australia's Telecommunications and Other Legislation Amendment (Assistance and Access) Act (TOLA) of 2018. In both cases, governments establish access requirements without imposing local storage obligations or restricting cross-border data flows. Firms are not required to keep data within national borders but must ensure that authorities can access relevant data when legally authorized. This may involve disclosing the location of stored data, maintaining records according to domestic standards regardless of storage location, or providing technical assistance to enable access to data stored abroad. While this model is less restrictive for cross-border data movement, it raises concerns about extraterritorial reach, the sovereignty of third countries, and the protection of personal data and confidential information.

Moreover, the physical location of digital infrastructure does not necessarily translate into domestic value creation or digital industrialization. In the digital economy, a large share of value is captured at the level of platforms, data assets, algorithms, and intellectual property, which are typically controlled by globally integrated firms and only weakly tied to the geographical location of servers. As a result, while localization may affect certain flows in national accounts, its capacity to reshape the underlying distribution of value in digital markets remains limited, especially in the absence of complementary policies in areas such as industrial policy, data governance, and competition policy.

At the same time, domestic laws governing data flows—whether enabling, restricting, or prohibiting them—directly affect the ability of states and firms to participate in the global economy. Measures that limit cross-border transfers or mandate localization have raised concerns that regulatory heterogeneity is contributing to digital market fragmentation (Evenett & Fritz, 2022). For firms, the resulting compliance costs and legal risks may lead to market exit or reluctance to expand internationally (Fritz & Giardini, 2023).

Ultimately, domestic approaches to data flows reflect a delicate balancing act between promoting public policy objectives, building local capacity, and reaffirming national sovereignty, while also seeking to reduce "data frictions"—the political and economic costs arising from conflicting data governance regimes (Azmeh et al., 2021). Regulatory interoperability and frameworks such as "Data Free Flow with Trust," a concept originating in Japan, launched at the G20, and currently developed within the OECD, offer one pathway to mitigate these frictions by promoting interoperability and risk-based safeguards.

Nevertheless, interoperability is not an end in itself. If pursued without a clear strategic orientation, it may reinforce data and value capture as well as market concentration. From a development perspective, some frictions may be necessary (Gurumurthy, 2026). For example, data-sharing agreements can be made conditional on certain development-oriented purposes, enabling more equitable models of data value creation and appropriation. The African Continental Free Trade Area (AfCFTA) Digital Trade Protocol (DTP) and the Annex on Cross-Border Data Transfers represent an initial step in this direction. Article 19 encourages, for example, certification systems for cross-border data transfers, and other specific data transfer mechanisms tailored to the needs of certain underrepresented groups (i.e., MSMEs, women, youth, Indigenous Peoples, among others). By aligning interoperability with development goals, countries may reduce harmful frictions while ensuring data remains a key resource for domestic innovation.

5.0 Data and International Trade Law: Existing and emerging rules

The importance of data to the global economy has prompted an evolution within international trade law. This section examines the legal frameworks that are relevant to data flows, analyzing both the established multilateral system and the more agile, innovative approaches emerging in PTAs and DEAs.

5.1 The WTO Framework

The influence of trade law on the development of the digital economy is significant. Within the multilateral trading system, some agreements have enabled data flows by liberalizing the basic infrastructure necessary for data-intensive economies to develop. For example, the Information Technology Agreement (ITA) and its expansion (ITA II) lowered tariffs on information and communications technology (ICT) goods, which enabled the acceleration of digitization. The General Agreement on Trade in Services (GATS) Annex on Telecommunications and its Reference Paper created a stable infrastructure foundation upon which digital trade and e-commerce depend, establishing the pro-competitive rules and non-discriminatory access to telecom networks. The triad of key WTO agreements—the General Agreement on Tariffs and Trade (GATT), the GATS, and the Trade-related Aspects of Intellectual Property Rights—forms the cornerstone of the global trading system and has influenced the development of the digital economy since the 1990s.

The GATS, in particular, is relevant to data-driven services and to discussions on cross-border data flows. Although disagreements in relation to "new services" and services classification still persist (Willemyns, 2021), the GATS provided a framework for the development of service sectors that currently rely heavily on data, such as computer services, audiovisual services, and telecommunications. In addition, it also sets the framework for the cross-border supply of traditional service sectors that have become tradable due to digitization and cross-border data flows.

Importantly, the GATS can apply to any government measure that directly or indirectly affects trade in services. This may include data flow restrictions that affect the supply of a service covered by the Agreement. This means that restrictions on transferring data across borders could violate existing GATS obligations if, for instance, they discriminate against foreign providers of digital services or restrict their market access. It should be noted, however, that the GATS applies with a caveat: while most-favoured nation (Article II) and transparency obligations (Article III) apply to all services, market access, national treatment and additional commitments apply only in sectors where countries have committed to opening their markets (Mishra, 2024). This creates loopholes in several situations in which countries may wish to introduce barriers to data flows at the domestic level.

5.2 Preferential Trade Agreements and Digital Economy Agreements

In spite of its relevance, the GATS—and the WTO legal architecture more broadly—predates the boom of the commercial Internet, and "legal adaptation" to the context of the digital economy has not happened under the WTO (Burri, 2017). This "has triggered forum-shopping—bilaterally, regionally, or through plurilateral initiatives" (Burri, 2017, p. 99). Many changes brought by the digital economy have influenced the search for regulatory solutions outside the WTO legal system (Burri & Polanco, 2019).

Most of the innovation in the regulation of digital trade, including when it comes to data flows, has been introduced via e-commerce and digital trade chapters in PTAs, and, more recently, in DEAs, which are a type of stand-alone agreement entirely and exclusively dedicated to measures affecting trade in the digital economy (Soprana, 2021). In September 2025, out of 477 agreements which were part of the Trade Agreement Provisions on Electronic Commerce and Data (TAPED) database, maintained by the University of Lucerne, 142 included dedicated digital trade or e-commerce chapters (Callo-Müller, 2025). There were also nine DEAs.

It is possible to classify the provisions in PTAs relevant to data and cross-border data flows in three groups: a) specific provisions on cross-border data transfers and data localization (Subsection 4.2.1); b) provisions that apply to data more broadly, which are likely to impact on cross-border data transfers (Subsection 4.2.2); c) new and emerging issues related to the data economy (Subsection 4.2.3).

Specific Provisions: Cross-border transfer of information and location of computing facilities

As the importance of cross-border flows to the digital economy grew, national regulations limiting the flow of data started to be seen as a significant digital trade barrier (Burri, 2017), prompting countries to adopt specific provisions seeking to remove obstacles to cross-border data flows. While non-binding provisions could be identified as early as 2000 in the Jordan–United States free trade agreement (FTA), stronger commitments started to be included later. The first binding provision on cross-border information flows is found in the 2014 Mexico–Panama FTA.

In subsequent years, U.S.-driven free trade agreements set the pace for the regulatory design of digital trade more generally and for provisions on cross-border data flows, more specifically (Burri, 2017; Gao, 2018). Since then, data transfer obligations have become one of the most important elements of modern digital trade agreements. In September 2025, 74 agreements (out of the 477 in the TAPED database) had provisions on cross-border data flows, and 44 agreements contained rules on data localization (Callo-Müller, 2025).

Binding provisions on "Cross-Border Transfer of Information by Electronic Means" or "Cross-Border Information Flows" were designed to facilitate data flows by limiting a country's ability to restrict them. These rules establish a baseline of openness, seeking to ensure that domestic data governance regulations do not create unnecessary barriers to digital

trade. Using positive or negative formulations (i.e., "Each Party shall allow the cross-border transfer of information by electronic means" or "A Party shall not prevent cross-border transfer of information by electronic means"), these rules seek to ensure unhindered cross-border data transfers.

Two variations found in the language of this baseline provision are worth noting. The first is whether the baseline provisions refer specifically to data transfers necessary for the conduct of digital trade, or, more broadly, to the conduct of business of a covered person. While the latter option is prevalent among most agreements, such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the Regional Comprehensive Economic Partnership Agreement (RCEP), the former has been adopted by the AfCFTA DTP.

The second language variation is whether personal data is explicitly included and expected to flow across borders without significant barriers. For example, the CPTPP affirms in Article 14.11 that "Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person." Similar language is adopted in DEAs, as can be exemplified by the United States–Japan Digital Trade Agreement, the Digital Economy Partnership Agreement (DEPA), and the AfCFTA DTP. Alternatively, RCEP, which also has a provision on Cross-border Transfer of Information by Electronic Means (Article 12.15), makes no specific reference to the flow of personal information.

In addition to provisions on cross-border transfer of data, most agreements also have provisions that prohibit the mandatory location of computing facilities. These provisions seek to prevent data localization, affirming that countries which are parties to the agreement shall not require firms to use or locate computing facilities in their territory as a condition for conducting business.

Provisions that promote the cross-border transfer of information and those that prohibit the mandatory location of computing facilities are closely interrelated. The first set of rules, which requires parties to allow cross-border data transfers, aims to minimize obstacles to the flow of data that is essential for digital trade. The second set, which prohibits forced localization, constrains the ability of states to require firms to maintain or use domestic data infrastructure as a condition for doing business.

This does not mean, however, that these provisions are logically equivalent: restrictions on cross-border data transfers do not automatically entail formal localization requirements, even if they may produce localization effects in practice. If transfers are subject to high compliance costs or regulatory uncertainty, firms face incentives to process data domestically in order to maintain service provision and manage legal risk, despite the absence of a legal obligation. In all cases, however, the decision to localize remains contingent on market size and the country's strategic importance. In smaller or less profitable markets, firms may instead limit services or exit altogether.

The case of Ireland within the European Union serves as an illustration. Although the General Data Protection Regulation does not mandate data localization, its stringent conditions on international transfers have led many global technology firms to establish substantial data

centre capacity within an EU member state in order to ensure seamless compliance, even in the absence of a formal legal requirement to do so. Ireland emerged as a preferred location due in part to its longstanding corporate tax incentives. Taken together, these dynamics illustrate that data localization emerges not only from legal mandates but also from the interaction of regulatory constraints and firm-level economic incentives.

The most salient and divergent aspect of provisions dedicated to cross-border transfer of information and provisions on location of computing facilities is not the baseline formulation, but the exceptions introduced to safeguard policy and regulatory space. In digital trade agreements, exceptions related to data transfers and localization can be horizontal or vertical. "General exceptions" and "security exceptions" are horizontal exceptions applying to the whole agreement, or specifically to the e-commerce chapter, where provisions on cross-border data transfers and location of computing facilities are located. These provisions are often modelled on, or explicitly reference, the general exceptions and security exceptions found in the GATT (Articles XX and XXI) and in the GATS (Article XIV and Article XIV *bis*).

Most PTAs do not make it clear whether they only borrow the textual architecture of exceptions from WTO law, or also intend to transplant the corresponding WTO jurisprudence.[5] Nevertheless, even without an explicit reference, WTO jurisprudence could be used in practice as an interpretative aid (Burri & Kugler, 2024). Within the WTO dispute settlement system, the legal threshold for successfully invoking general exceptions in disputes is high because it involves several complex legal tests. The panels and the Appellate Body must consider: a) whether the measure falls within the scope of one of the listed objectives in the exception; b) if the measure is necessary to address the relevant public interest at issue, with a sufficient nexus between the measure and the objective pursued; c) whether the measure fits the conditions established in the chapeau of Article XIV GATS/Article XX GATT, and is not arbitrary, unjustified, and a disguised restriction on trade. While countries frequently succeed at proving necessity, they often fail at meeting the conditions established in the chapeau. As a result, "these exceptions and the tests developed thereunder set a relatively high hurdle for WTO members, and the 'success rate' for passing them in case of a disputed measure has been rather low" (Burri & Kugler, 2024).

Faced with these constraints, many countries also include vertical exceptions directly within data flow and localization provisions, seeking to secure more predictable and robust protection for legitimate public policy objectives, without having to rely solely on general exceptions. In the case of provisions on data flows and location of computing facilities, vertical exceptions may either:

- adopt a specific formulation, such as an exception to cross-border transfer of information and to the location of computing facilities aimed at protecting a specific policy goal. The RCEP, for example, adopts a broadly framed, self-judging security exception, which provides maximum regulatory autonomy for the state invoking it,

[5] A notable exception is the Korea–Australia FTA, which states explicitly in its Chapter on Dispute Settlement that: "Where an obligation under this Agreement is identical or substantially identical to an obligation under the WTO Agreement, the panel shall adopt an interpretation which is consistent with any relevant interpretation established in rulings of the DSB [Dispute Settlement Body]."

but generates a high degree of uncertainty for trading partners. In this case, regulatory autonomy is given precedence over predictability.

- adopt a broad formulation, allowing parties to adopt or maintain measures inconsistent with the baseline provision to achieve a legitimate public policy objective. In this case, regulatory autonomy is mitigated by the need for predictability, since the exception is subject to explicit conditions, including necessity-type requirements, non-discrimination, and proportionality (i.e., provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade, and does not impose restrictions greater than required to achieve the objective).

Until recently, there were few examples of provisions on data flows and location of computing facilities binding LDCs, and developing countries more generally (Banga et al., 2021). This scenario started to change with the introduction of the AfCFTA DTP. Adopted in February 2024, the AfCFTA DTP is the largest digital trade agreement in terms of participating countries. It is also the largest South–South digital trade agreement, as all state parties are developing countries or LDCs—potentially, over 30 LDCs may ratify this agreement. The AfCFTA also innovates by adding more detailed provisions and some different commitments on data flows and localization, when compared to other agreements.

Box 1. In focus: The AfCFTA DPT and the Annex on Cross-Border Data Transfers

The Annex on Cross-Border Data Transfers to the AfCFTA Protocol on Digital Trade has some very notable features. First, the Annex is a cornerstone of data governance more broadly. Although titled "Cross-Border Data Transfers," the Annex holistically supports all data-related provisions in Part IV of the AfCFTA DTP (Sucker, 2025), namely: cross-border data transfer (Article 20), personal data protection (Article 21), data facility location (Article 22), and data innovation (Article 23).

Part III of the Annex, titled "Facilitating Cross-border Data Transfers" (Articles 16–22) has some provisions that innovate and expand on how this particular issue is tackled by traditional agreements. For example, Article 16 on "principles for cross-border data transfers" creates an additional responsibility for parties to "adopt or maintain reasonable and appropriate measures to ensure that cross-border data transfers, including personal data, by persons of State Parties for the conduct of digital trade are uninterrupted and secure" (Article 16.3), and to proactively "identify and remove barriers" to cross-border data transfers (Article 16.5). Moreover, Articles 17 and 18 establish, respectively, obligations to accord an equivalent level of protection to data transferred by a person from another state party, as well as an obligation of non-discrimination.

A significant innovation appears in Article 19, dedicated to "Cross-Border Data Transfer mechanisms." While agreements often seek to encourage data transfers, developing countries and LDCs grappling with insufficient infrastructure may find it hard to operationalize such provisions. Article 19 provides examples on how to pull together regional resources by mentioning regional data centres and cloud systems (including for disaster recovery), the development of industry-specific self-regulatory data codes

of conduct, certification systems for cross-border data transfers, and other specific data transfer mechanisms tailored to the needs of certain underrepresented groups (i.e., MSMEs, women, youth, Indigenous Peoples, among others). The article also establishes important principles, such as transparency and interoperability, and calls for the involvement of other stakeholders in its implementation.

Article 21 calls for cooperation among state parties on a range of activities, from research, capacity-building, and technical assistance to regulatory cooperation among authorities. In Article 22, parties commit to a series of actions focused on unlocking the value of data for development.

The AfCFTA's Cross-Border Data Transfer Annex provides an example of "economic regionalism" (Cai, 2010; Kassa, 2025), seeking to strike a balance between nationalist data policies and broader global integration. By fostering regional cooperation and pooling resources, it represents an innovative, development-oriented approach to data governance. If well implemented in future, this framework may allow the continent to forge its own path, using coordinated data flows as a catalyst for regional economic integration and growth.

Provisions That Apply to Data More Broadly That Are Likely to Impact Cross-Border Data Transfers

In the context of digital trade agreements and e-commerce chapters, there are provisions that, while not explicitly regulating cross-border data transfers, establish critical frameworks that directly shape and constrain them. By setting rules for how data must be handled in general, these broader obligations inevitably influence the feasibility, incentives, cost, and structure of international data flows. Specifically, we analyze three key areas: a) protection of personal information; b) open government data; and c) data innovation.

Provisions on Personal Information Protection

Completing an online transaction requires sharing personal data, often with goods and service providers across borders. This creates a link between digital trade and the laws enacted at the domestic level for the protection of personal data, which in turn establishes the foundational rules for these international data flows. The intrinsic connection between data privacy and trade was acknowledged in foundational instruments like the OECD Privacy Guidelines and the Asia-Pacific Economic Cooperation Privacy Framework.

In contemporary digital trade agreements, this link is operationalized through three core types of provisions: those governing data protection, cross-border data transfers, and data localization. This section focuses on the first category.

Robust personal data protection is a critical enabler of trust in e-commerce and digital trade, a fact increasingly reflected in treaty practice. By September 2025, provisions on privacy and data protection appeared in 158 of the 477 agreements catalogued in the TAPED database (Callo-Müller, 2025). The nature of these provisions has evolved significantly. Early treaty language was often simple and non-binding, whereas modern agreements demonstrate a

clear trend toward greater complexity and specificity, detailing substantive principles and obligations for protecting personal information.

It is possible to identify three dominant templates for personal privacy protection in trade agreements (Bradford, 2023; Callo-Müller, 2025): a) an open or liberal model, inspired by the U.S. framework as reflected in the CPTPP, which prioritizes data flows and commercial interests; and b) a rights-oriented model, centred on the protection of privacy as a fundamental right, as championed by the EU. This template varies, however, displaying a strong articulation in agreements like the EU–New Zealand FTA or a more tempered version in the later EU–Singapore FTA, which omits explicit references to fundamental rights; 3. An Asian model, typified by the RCEP, which establishes binding provisions but deliberately excludes the entire e-commerce chapter from formal dispute settlement, thereby limiting their enforceability.

Provisions for personal information protection in digital trade agreements typically converge around some core features:

- a foundational recognition of data protection's value in fostering trust and confidence in digital commerce and, in some frameworks, as a fundamental right;
- a binding commitment for parties to adopt or maintain a domestic legal framework for data protection, while acknowledging divergent legal approaches. Some agreements, like the AfCFTA DTP, also feature softer commitments (i.e., a "best endeavour" clause on establishing data protection authorities in Article 21);
- references to key international standards (i.e., the OECD Privacy Guidelines or established data protection principles) that parties should consider when developing their legal frameworks;
- commitments to apply data protection laws in a non-discriminatory manner;
- transparency obligations, such as publishing information on compliance procedures or available remedies;
- a stated objective to promote compatibility between different regimes through mechanisms like adequacy decisions or mutual recognition;
- various interpretative or operational provisions (often found in footnotes or annexes) that accept multiple implementation pathways (i.e., comprehensive laws, sectoral rules, or self-regulation, as noted in the CPTPP), and that may offer special and differential treatment for LDCs.

Modern privacy provisions in trade agreements serve to manage the data frictions created by conflicting national regimes. By seeking to promote interoperability while accommodating legal diversity, they aim to reduce the costs and uncertainties of cross-border data flows.

Provisions on Open Government Data

Open government data (OGD) can be understood as data produced, collected, or funded by the government or public institutions that is publicly available and that presents the technical and legal characteristics necessary for it to be freely used, reused, and redistributed.

From a public policy perspective, OGD plays an important role in supporting data-driven policy-making and in strengthening participatory governance by enabling access to information and fostering informed civic engagement. From an economic perspective, OGD generates economic value by fostering innovation and supporting data-driven industries that leverage open data to develop new products and services.

Crucially, OGD also functions as an indirect enabler of cross-border data flows. By mandating the standardized, machine-readable publication of high-value data sets (i.e., geospatial, transport, or meteorological data), OGD policies create global pools of interoperable information. This reduces technical and informational barriers, allowing firms and researchers worldwide to access, transfer, and build upon public data, thereby stimulating international data circulation and economic activity.

As a consequence, OGD has become a recurring feature in digital trade agreements. The text of baseline provisions on OGD varies, but there is often a recognition that facilitating public access to and use of government information may foster economic and social development, competitiveness, and innovation. This is accompanied by a commitment, often based on best-effort wording, to make government information and data available in an open and machine-readable format.

Some key characteristics of these provisions include the following:

Broad Scope

Some agreements frame OGD within wider commitments to "open public information," explicitly listing data as a core component (i.e., DEPA Article 9.5, Items 1 and 2).

Soft Obligations

Language often employs "best-effort" terms such as "shall endeavour" and "shall endeavour to ensure […] to the extent practicable," creating a softer commitment, rather than a higher level of obligation.

Technical Interoperability

Most agreements include machine-readable and open-format requirements. This is one of the most recurrent and actionable elements from OGD provisions, aiming to enable data reuse.

Cooperation Mechanisms

Some agreements encourage cooperation and mutual learning among parties. DEPA provides an emblematic example of a detailed provision in this regard. In addition, the Joint Statement Initiative (JSI) Agreement on Electronic Commerce (stabilised text) also encourages parties "to expand the coverage of such data, such as through engagement and consultation with interested stakeholders." This language appears in other agreements, such as the UK–New Zealand FTA (Chapter 15, Article 15.17).

Commercial Reuse

Some agreements explicitly promote the commercial reuse of OGD, particularly to create opportunities for MSMEs (e.g., Canada–United States–Mexico Agreement, JSI Agreement on E-commerce).

Essential Carve-Outs

Provisions safeguard the right to withhold data for reasons of privacy, confidentiality, and national security.

OGD provisions in trade agreements reflect a strategic effort to leverage public sector information as infrastructure for the digital economy, stimulating innovation and competitiveness, and influencing the broader architecture of cross-border data flows.

Although the value of OGD for innovation and competitiveness is broadly recognized, there may also be an uneven distribution of OGD benefits. Actors with the resources to aggregate and combine OGD with proprietary data sets may capture disproportionate value accruing from open data, raising concerns that OGD could entrench rather than reduce market concentration (Kruse & Grafenstein, 2025).

In response, there is a growing concern with data-sharing responsibilities for the private sector and data equity. Some jurisdictions are exploring legally mandated data-sharing frameworks, reciprocity-based licensing terms (which require, in certain situations, private actors to share data back with the public), as well as tiered access regimes designed to balance data openness with equity safeguards. An example is the EU's Data Act, which introduces some mandatory data-sharing obligations for private actors under FRAND terms. In New Zealand, a Supreme Court decision recognized Māori custom as common law, providing a legal basis for the sovereignty of the Māori over their data.

Provisions on Data Innovation

Data innovation provisions in modern digital trade agreements represent a significant shift: they move beyond the traditional goal of simply removing barriers to data flows and focus on establishing proactive, collaborative frameworks to unlock the economic and social value of data. Such provisions can be found in DEPA and in the AfCFTA DTP, for example.

The strategy to promote data innovation is twofold. First, these provisions encourage the creation of trusted, interoperable environments for data sharing, such as through regulatory sandboxes (explicitly endorsed in both DEPA Article 9.4 and AfCFTA DTP Article 23). These sandboxes allow businesses and researchers to test new data-driven products and services, including those involving cross-border personal data, within a controlled regulatory space, thereby demonstrating concrete benefits while managing risks.

Second, they commit parties to collaborative development of foundational policy and regulatory approaches, including policies for harmonizing standards, data mobility and consumer data portability (AfCFTA DTP 23.b, DEPA 9.4.2), the creation of data-sharing frameworks that protect personal information (AfCFTA DTP 23.d), and open licensing agreements. Third, they associate these technical and regulatory enablers to the pursuit of

certain policy goals, such as innovation, competition, and market efficiency, the diffusion of information, knowledge, research, technology, culture, and the arts. Parties to the AfCFTA DTP, in addition, set an explicit goal of taking advantage of data-reliant technologies and services to support the development of their countries and their citizens.

Ultimately, these provisions recognize that the benefits of data flows are not automatic. They must be cultivated through shared infrastructure, legal foundations, and deliberate efforts to ensure all parties have the technical and governance capabilities to participate in and benefit from the data-driven economy.

Box 2. Data-related provisions in the JSI Agreement on Electronic Commerce

At the beginning of negotiations, cross-border data flows were a central item on the agenda of the JSI. Nevertheless, the text of the Agreement on Electronic Commerce does not include rules on cross border data flows and on the location of computing facilities. These issues were ultimately left out because of divergent views and sensitivities among JSI participants. In particular, the United States withdrew its support for rules on data flows, data localization, and source code, arguing that these issues require more nuanced treatment and domestic regulatory space. The lack of obligations on cross-border data transfers or localization does not mean, however, an absence of data-related provisions. The Agreement has specific commitments in two of the areas selected for analysis in this section: personal data protection (Art. 16) and OGD (Art. 12).

In relation to personal data protection, the text recognizes that strong and effective protection of personal data contributes to enhancing consumer confidence and trust in the digital economy. Parties commit to adopting or maintaining a domestic legal framework that provides for the protection of the personal data of users of electronic commerce. Very importantly, a footnote determines that a party may comply with this obligation by adopting or maintaining measures, or a combination of measures, such as a comprehensive privacy law, personal data protection laws, sector-specific laws covering privacy or other laws that address privacy violations. This non-exhaustive list aims to accommodate different domestic legal approaches to data protection and gives parties significant flexibility on how to fulfill the main obligation contained in this section. Other commitments (of a "best-effort" nature) relate to non-discrimination in the application of data protection laws, transparency obligations, and the goal to promote legal compatibility.

With regard to OGD, the text of the Agreement is extensive and detailed. It encourages parties to make government-held data (which is not restricted under domestic law) digitally available for public access and use (best-effort language), emphasizing that such openness can foster innovation, competitiveness, and inclusive economic development. Moreover, parties shall endeavour, to the extent practicable, to ensure that such data is machine-readable, searchable, timely, accompanied by standardized metadata, and that access is provided at minimal cost. In parallel, parties should avoid undue restrictions on reuse, redistribution—for commercial or non-commercial purposes—including in the process of producing a new product or service.

Parties are encouraged to cooperate in order to facilitate and expand public access to and use of OGD, with a view to encouraging the development of electronic commerce and creating business opportunities, particularly for MSMEs. Although the Agreement does not have a separate section on data innovation, this latter aspect hints at the importance of unlocking the economic and social value of data.

New and Emerging Digital Trade Topics Related to the Data Economy

Several provisions that can be found in more modern trade agreements have shown an intimate interplay with data governance and data flows. The TAPED project codebook clusters these provisions under the label of "new data economy issues"[6] (Burri & Callo-Müller, 2025), a categorization that reveals their deep, structural dependency.

This dependency exists because the governance of data—including rules on its cross-border flow—serves as the foundational infrastructure for the modern digital economy. Provisions on data are intimately linked to nearly all emergent "new data economy" issues. This connection operates through three primary channels, since data simultaneously serves as an essential enabler for specific technologies; as a determinant of market structure and access; and as a critical prerequisite for equitable participation in the digital economy.

First, data serves as an enabler because it is the raw material for advanced digital technologies. For example, the development and deployment of AI and financial technology (fintech) are dependent on rules governing data access, quality, and transfer. AI algorithms require vast, often cross-border, data sets for training, making innovation contingent on predictable data flow rules. Similarly, fintech services depend on secure and standardized mechanisms for data sharing and portability. In addition, foundational digital public infrastructures, such as digital identity systems, as well as tools for legal technology (Lawtech), cannot achieve security, interoperability, or user buy-in without robust underlying frameworks for data protection and processing, in order to guarantee trustworthy data flows.

Second, rules on data directly shape market structure and access, making them a core concern of digital competition (Burri, 2019; Larsson, 2021). Competition policy in the digital economy is increasingly focused on data concentration as a source of market power. Provisions that promote data portability, interoperability, and standardization are direct regulatory tools to lower entry barriers and foster a more competitive landscape. This rationale can also be extended to public sector efficiency: provisions seeking to enable government procurement through electronic means rely critically on standardized data formats and secure transmission protocols to ensure transparency and interoperability across systems and borders.

[6] There are 10 types of provisions clustered under this label, namely: 1. Competition policy related to the digital economy; 2. Digital identities; 3. Digital inclusion; 4. Fintech; 5. AI; 6. Provision allowing government procurement, including by use of electronic means; 7. Provisions that promote or recognize the need for standardization, interoperability or mutual recognition regarding digital means; 8. Lawtech; 9. Public domain; 10. Fostering digital talents or digital skills.

Finally, effective data governance is a prerequisite for equitable participation in the digital economy. Goals of digital inclusion are undermined if individuals, communities, or MSMEs lack the skills or infrastructure to control and extract value from data. Proactive governance choices, such as dedicating certain data sets to the public domain, can stimulate innovation. As a consequence, initiatives for fostering digital talents and skills must become an integral part of national development policies, receiving support from all stakeholders, as mentioned by Article 33 of the AfCFTA DTP.

Most of these provisions tend to appear as best endeavour, cooperation-oriented, or aspirational clauses, since they relate to emerging policy areas, which are fast-paced and where governments want flexibility. Nevertheless, some agreements contained hard provisions, such as DEPA's provisions on fintech, which establish that parties "shall" promote cooperation between their fintech industries and promote fintech solutions.

Above all, provisions on "new data economy issues" point to a growing interface between digital trade law and the broader realm of digital governance, with data governance serving as a bridge between the two regulatory realms. The development of the digital economy and of digital governance may be decisively shaped by the legal and policy choices embedded in trade agreements, influencing which actors can participate, which business models can scale, and ultimately, how the value generated by the global data ecosystem is allocated.

6.0 Development Considerations

A growing consensus warns that the wealth generated by the digital economy is becoming increasingly concentrated in a handful of countries and corporations. Multiple reports from organizations such as the World Bank (2016), the Internet Society (2019), the World Economic Forum (2021), and UNCTAD (2021) highlight a persistent trend of market and technological consolidation. This dynamic is widening the digital divide and exacerbating inequalities between developed and developing economies (Morosini et al., 2024).

The unbalanced nature of this growth is evident in trade data. While digitally deliverable services now constitute 56% of global services exports (up from 49% in 2015), their share in LDCs has remained stagnant at around 16% (UNCTAD, 2025). Similarly, the combined share of Africa and Latin America in global ICT services exports has declined from 3.3% to 2.5% over the same period, indicating a marginalization of key regions in this sector.

This economic divergence is compounded by a geopolitical reorientation of trade. As the 2023 WTO World Trade Report notes, commerce is increasingly aligning along geopolitical considerations (WTO, 2023), putting pressure on developing countries to position themselves along the fault lines. The simultaneous fragmentation of both value chains and political ideologies risks entrenching global divides. In this environment, development priorities are increasingly eclipsed by geopolitical and geoeconomic concerns, making it harder to advance inclusive growth.

Developing countries face a complex set of interlinked domestic and international challenges in their quest for equitable participation and long-term development in the digital economy, as discussed below.

6.1 The "Data Divide" and a Situation of Asymmetrical Value Capture

Data-related divides have special explanatory relevance to understand the growing gap between developed and developing countries because they are "the 'intangible asset[s]' and 'infrastructure' underlying the digitalised economy" (Mishra, 2024). The importance of data is highlighted not only by its centrality to the economy and to digitalized societies, as discussed in Section 2 of this paper, but also by the fact that it underpins all aspects of the "new data economy"—from fintech to AI—discussed in Subsection 4.3. This means that lack of access to data and limited capacity to harness its value help explain patterns of concentration, as well as to foresee obstacles in the path to development.

Low levels of access to data confine developing countries to a "data poverty trap" (Farboodi & Veldkamp, 2021), with lower levels of production and transactions and lower profits, hindering further data accumulation and analysis. This helps explain concerns about data colonialism (Chander & Sun, 2023) among developed countries, who fear becoming providers of raw materials (now in the form of data) and markets for digital products and services, yet lacking the means to effectively narrow the gap and move up the value chain.

Digital trade law has played an important role in making "free cross-border data transfers" a policy and regulatory default by putting an emphasis on "trust" and the development of certain safeguards. Nevertheless, without prioritizing equity and data justice in digital trade relations, developing countries often become net exporters of raw data, while remaining importers of high-value data-driven services and technologies. This dynamic can lead to a form of digital value extraction, where the economic benefits and innovation derived from data are captured by foreign platforms and firms, with limited domestic spillovers.

6.2 Negotiating From a Position of Structural Asymmetry

Current asymmetry in the digital economy is mirrored in the negotiating arena (Ismail, 2021). Developing countries frequently engage in digital trade discussions where the framing and the default templates of provisions are set by advanced digital economies (Burri, 2017; Morosini et al., 2024). This creates pressure to adopt rules designed for different stages of development, often without the necessary domestic institutional capacity to implement them effectively or to leverage them for national gain, locking developing countries in disadvantageous positions.

6.3 The Openness-Policy Space Dilemma

A central challenge in digital trade negotiations lies in balancing openness and potentially advantageous integration in the global trading system with regulatory autonomy. Overly restrictive measures, such as broad data localization, can stifle investment, increase costs, and cut off access to global digital services. Conversely, a lack of domestic regulation may also have negative economic consequences and undermine legitimate public policy objectives. Finding this balance requires a case-by-case assessment for each country, while defending it in trade negotiations requires sophisticated regulatory foresight and a good understanding of the policy space other negotiating parties have to engage in coalition building. This kind of strategic intelligence is difficult to muster under resource constraints and negotiating pressure.

6.4 The Gap Between Commitments and Implementation Capacity

A central challenge for developing countries in digital trade negotiations is the persistent mismatch between the binding commitments they undertake and the practical capacity required to implement them. While it may be advantageous for a country to engage with ambitious provisions, the institutional, technical, and human resources needed to operationalize those rules are often underdeveloped. Current agreements typically address this imbalance through non-binding mechanisms, such as "best endeavour" clauses for capacity building or the provision of extended transition periods for compliance. However, these tools frequently prove inadequate. Transition periods merely delay the inevitable compliance burden, while "best-effort" commitments are too vague and unreliable. This implementation gap risks creating a two-tier system in which the benefits of digital trade agreements remain out of reach precisely for those countries that need them most.

6.5 The Foreclosure of Traditional Development Pathways

True economic advancement has historically been driven not merely by the exchange of goods and capital, but more fundamentally by the transfer of knowledge and technological prowess (UNCTAD, 2014). This dynamic typically involves a directional flow from core innovation hubs toward nations with less mature scientific and technological infrastructures. To actively capture these benefits, states have long deployed strategic policy interventions aimed at accelerating technology transfer. However, the scope for such national policy action has been sharply curtailed (UNCTAD, 2014). Over the years, many previously accepted instruments, including various performance requirements, have become largely off-limits due to the legal constraints embedded in contemporary international economic agreements.

In the digital domain, this foreclosure is compounded by specific provisions on cross-border data flows. The movement of data is the lifeblood of modern technological diffusion, yet rules that mandate its unfettered transfer can paradoxically hinder deep technology transfer. When data can be transferred and processed seamlessly across borders, firms face weaker incentives to internalize advanced computing, analytics, and research activities within host economies, particularly where regulatory or market conditions do not otherwise favour local investment. Consequently, the potential for local spillovers, tacit knowledge exchange, and the development of domestic high-skill ecosystems is significantly diminished.

The architecture of digital trade rules presents a critical dilemma. While provisions that facilitate cross-border data flows enable participation in the global digital economy, they can simultaneously solidify a pattern of technological dependency. This dynamic shows that in the absence of complementary industrial, regulatory, and infrastructural policies, the liberalization of data flows alone is an insufficient foundation for development.

At the same time, although many of these agreements formally appear to foreclose traditional industrial policy instruments, recent practice indicates a partial reopening of policy space, as major actors, notably the United States and the EU, increasingly deploy such instruments openly (Manak, 2025). This suggests that the scope of permissible state intervention is shaped not only by treaty disciplines but also by shifting political signals and prevailing interpretations of what constitutes a legitimate measure. These elements can be influenced and transformed.

6.6 The Geoeconomic Imperative: Data governance as economic security

Data governance is increasingly driven by geoeconomic competition and economic security considerations. Major economies are reframing their approach to data flows, as exemplified by the U.S. administration's 2023 decision to withdraw its support for proposals on cross-border data flows, data localization, and source code in the context of the WTO JSI negotiations on e-commerce. While the justification provided by the United States related to preserving "enough policy space" for discussions on these issues to unfold at the domestic level (United States Trade Representative, 2023), the decision should also be understood in the context of geopolitical competition. The interweaving of geopolitics and geoeconomics leads to a growing number of limitations to the cross-border flows of an ill-defined pool of "important data" or

"critical data" (Giovane et al., 2023), in order to protect competitiveness and resilience from risks and strategic dependencies.

For developing countries, this introduces a complicating element: they must navigate a landscape where data flows are restricted not to foster "trust" safeguards (i.e., equivalent levels of data protection), but for techno-nationalist rivalry, de-risking, and strategic containment. This securitization (Buzan et al., 1998) fragments the digital/data economy into competing blocs, heightens compliance costs, and can constrain policy choices, since adopting technologies or partners may trigger security concerns from powerful allies. Consequently, the challenge shifts from safeguarding the conditions to access and benefit from the global digital economy to surviving (and thriving) within a global economic order that is being actively weaponized by its largest players.

Box 3. In focus: Specific challenges for LDCs and vulnerable states

From the perspective of LDCs—particularly small, island, landlocked, or infrastructurally deficient states—these challenges are most acute. In some countries, unreliable energy supply and limited connectivity are still significant barriers to the development of digital infrastructure. This means that data cannot be processed locally, making "raw data export" the most viable option in the short term. Weak digital economies and underdeveloped domestic regulatory frameworks lower incentives for foreign direct investment (FDI) and for localizing data-intensive services, reinforcing the trend of value extraction.

However, some LDCs also possess distinct structural advantages that can be leveraged. In the case of island states, geography often orients them naturally toward services. Many LDCs have made progress in establishing the enabling conditions for digital development. Regulatory frameworks for e-transactions, for example, have advanced in many countries, creating legal predictability for digital trade and domestic e-commerce. This suggests that targeted investment, international cooperation and capacity building could help to nurture agile and specialized digital economies.

LDCs have small markets and little leverage to demand exceptions or special provisions in trade negotiations, but they could benefit from provisions that bind commitments to capacity-building and technical assistance. For some countries, membership in institutions, such as the Commonwealth, could be leveraged for additional technical cooperation, including to help these countries determine specific needs and to craft development-promoting actions and time frames. Whenever possible, institutional bodies and informal coalitions could be mobilized to promote the need for technology transfer, coordinate regulatory harmonization, and amplify the voice of LDCs in trade negotiations. International cooperation remains essential to preserve the flows of capital and technology that would be essential to meet the UN's Sustainable Development Goals.

Overcoming marginalization requires not merely flexibility within specific agreements, but a rethinking of the rules themselves. In this scenario, the digital trade architecture does not merely disadvantage the most vulnerable countries; it risks codifying and locking in their peripheral position in the global economy.

7.0 Policy Considerations

The global economic order is in a period of profound rebalancing (Stubb, 2025). Economic liberalism is waning, financial support for development is dwindling, and the rules-based trading system is under strain. This disruption coincides with the rising economic influence of non-Western nations and Global South blocs (Eisentrout, 2025). This dual shift creates uncertainty, but also a strategic opening for developing countries to renegotiate the foundational rules that paved the way for the development of the digital economy, including the possibility to contest the current trend of data accumulation and unequal extraction of value.

Seizing this opportunity is key. Without a proactive and coherent digital agenda, developing countries risk becoming collateral in great-power rivalries and targets of economic and political coercion in a world of deepening geoeconomic confrontation and resurgent protectionism. The alternative may lie in reinforced regionalism, South–South cooperation, and a coordinated diplomatic effort to recentre the digital trade agenda around development, including access to technology and data. This concerted action may create an opportunity to transform systemic upheaval into a lever for a more equitable digital economy.

In digital trade law, a glimpse of the kind of resolve that may engender collective action can be noticed in provisions encompassed in the AfCFTA DTP, and in a few development-oriented provisions in DEAs, which seek to highlight the importance of data for innovation, technology transfer, and to support MSMEs. These provisions merit a thorough implementation plan so they can serve as a stepping stone to more ambitious commitments.

Given the significant disparities in levels of development, economic structure, and digital capacity among developing countries and LDCs, and also within these two groups, a uniform "one-size-fits-all" approach is neither feasible nor desirable. Each country must assess its unique circumstances and strategic objectives, and calibrate its approach based on these reflections. The following points are therefore offered not as definitive recommendations, but as considerations for policy-makers and trade negotiators navigating the complex interplay between data governance, digital trade law, and domestic development.

7.1 Data Divide and Asymmetrical Value Capture

Tackling this problem requires coordination between different policy areas, such as trade, investment, competition policy, and industrial policy. Despite the silos within public administrations, there is a pressing need to create channels for transversal dialogue to enable a holistic approach to data. This dialogue can help overcome the unrealistic binary choice between free data flows versus forced data localization that has captured the attention of digital trade negotiators. A country's approach to cross-border data flows should be forged upon a solid understanding of its capacity to engage in data value chains in the present, and the position it realistically wishes to occupy in those value chains in the future. As discussed in Section 2, data is valuable insofar as it is a source for information, knowledge, and wisdom. The transformation of data entails several steps in the data value chain, such as data generation/collection, storage, processing and analyzing, and its embodiment into data-intensive products and services (Azmeh et al., 2021). Each stage has distinct economic

characteristics, barriers to entry (capital, skills, infrastructure), and potential for value addition, and it is important to have a sectoral assessment of where and how a country can viably specialize and capture value. This may not only guide a country's approach toward cross-border data flows, but also to investment attraction.

7.2 Regionalism as a Potential Path to Mitigate Structural Asymmetry

Global South nations are forming new trade alliances and partnerships not centred around traditional Western markets, like the United States and the EU. The importance of regionalism in digital trade is not new: the EU, for example, focused on promoting free flows of data internally, and used the size of its market as leverage, not only in negotiations, but also for regulatory influence (i.e., the "Brussels effect"). The upcoming Association of Southeast Asian Nations Digital Economy Framework Agreement and the AfCFTA DTP provide important examples of regionalism within developing regions. The AfCFTA DTP, in particular, fosters cross-border data flows within the continent, while also encouraging parties to the agreement to pull together regional resources to support infrastructure, such as data centres and cloud systems. Joint resources could also promote capacity building targeted at assisting countries in shaping policy and regulatory alternatives to the default templates of provisions set by advanced digital economies in trade negotiations. Ultimately, regionalism could serve as a building block for South–South coalition building, allowing developing countries to better coordinate positions, share technical analyses and model provisions that reflect common development interests.

7.3 Navigating the Openness-Policy Space Dilemma

The balance between openness and policy space is being put into question by developed countries, which are increasingly resorting to the loosely defined policy goals of "national security" and "economic security" to justify trade restrictions. In this context, developing countries have an opportunity to revisit their own understandings of the balance between openness and policy space. For example, developing countries and LDCs could benefit from negotiating more targeted and operationally useful exceptions in digital trade rules. This could include vertical exceptions to specific sectors or provisions in the agreement (i.e., cross-border data transfers and data localization) designed to support development objectives. When combined with capacity-building and technical assistance for implementing positive obligations (see Section 6.4), these exceptions may help countries preserve meaningful policy space.

7.4 Linking Rules to Implementation Resources

There could be a closer link between digital trade rules and implementation support. When negotiating PTAs, developing countries should explicitly tie commitments to concrete and enforceable capacity-building and technical assistance. Provisions should be binding, detailed, and focused on building the institutional, human, and technical capacities necessary to operationalize agreements effectively. This requires moving beyond vague "best endeavour"

clauses toward clearly specified commitments on funding modalities, expertise transfer, infrastructure development, and implementation sequencing. A useful illustration is the Investment Facilitation for Development Agreement, which couples binding disciplines with structured technical assistance and capacity-building provisions. It allows developing countries and LDCs to calibrate implementation timelines and provides for monitoring through reporting and review processes, offering a model in which commitments and implementation support are formally coordinated through sequencing, needs assessments, and transparency mechanisms.

7.5 Navigating Uncertainty in Development Strategies

Promoting development requires the transfer of knowledge and technology. A necessary starting point is investment in domestic absorption capacity, since deeper learning depends not only on exposure to foreign technological "spillovers" but also on the local capability to interpret, integrate, and innovate upon them. At the same time, development strategies must be reconsidered in light of a changing international context. While there could be a reopening of some policy space (as discussed in relation to industrial policy), there are also new constraints to the policy options available to developing countries. Official development assistance is under strain, FDI is volatile, and investment screening for national and economic security reasons could mean that investment in dynamic technology sectors could be directed to traditional regions to hedge against geopolitical concerns. Some countries with sizable markets and high return rates on investment may seek to reopen previously foreclosed development paths, such as performance requirements or technology transfer obligations. In parallel, smaller or more vulnerable developing economies may need to identify other strategies, such as South–South cooperation, or public–private innovation, that can be leveraged to support deep learning, even under conditions of geopolitical constraint, supporting business activities that share knowledge, not just extract data (see point 6.1).

7.6 The Place for Development in the Current "Geoeconomic" Turn

Three major players—the United States, China, and the EU—are, for different reasons, fuelling a geoeconomic turn that places economic security at the centre of concerns. These countries are major trading partners and sources of FDI for numerous developing countries, so their decisions will have ripple effects for their developing counterparts (Weinhardt & de Ville, 2024). For example, as global value chains reorganize following geopolitical constraints, they often become longer and more complex, with certain countries enhancing their participation by acting as intermediaries. Some developing countries may benefit from this restructuring. Mexico, for instance, became the U.S.'s main trading partner, partly due to the U.S.'s nearshoring goals. However, these changes could also hinder the inclusion of developing countries in higher and more complex levels of value chains, particularly of countries that are not geographically close or do not align neatly with politico-ideological alliances or notions of "like-mindedness." Export controls are becoming a central mechanism through which these constraints operate. By restricting access to critical and emerging technologies—such as semiconductors, advanced manufacturing equipment, or AI model weights—export controls

can limit the technological capabilities of developing economies and reduce the scope for industrial upgrading. In this evolving scenario, the role of trade negotiators has become more complex, but also increasingly important. While the core functions of trade and investment promotion remain unchanged, evaluating opportunities and challenges has become more difficult because the evaluation no longer strictly adheres to established criteria, such as tariff rates, trade complementarity, and the ease of doing business and investing. More than ever, diversifying partnerships is essential, particularly through South–South cooperation (point 6.2). In a scenario like this, it becomes crucial for countries to ground their actions in fact-based reasoning and capacity building that caters to just-in-time needs.

8.0 Conclusion

The governance of data flows sits at the intersection of digital transformation, economic integration, and individual and collective rights. The international trade law framework is adapting to the centrality of data, but this adaptation is occurring unevenly through PTAs and DEAs that reflect differing legal traditions, policy priorities, and levels of development. Underpinning these variations is a persistent tension between harnessing the economic benefits of integrated data flows and preserving the policy space necessary to pursue legitimate public objectives.

For developing countries and LDCs, navigating this terrain requires strategic clarity. The structural asymmetries that characterize the data economy will not be corrected by trade rules alone. These rules must be embedded within a broader national strategy encompassing digital infrastructure, skills development, competition policy, and support for MSMEs. Yet, trade rules are important: they can either lock in peripheral positions within global data value chains or be crafted to create openings for more equitable participation. The path forward lies not in an unrealistic binary choice between unfettered flows and mandatory localization, but in calibrated approaches grounded in domestic priorities and robust regional cooperation. Internationally, developing countries must continue to champion the development dimension in all trade forums. The rules of the global digital economy must actively support—not merely permit—their development and equitable participation in the digital economy.

References

Aaronson, S. (2018). Data is different: Why the world needs a new approach to governing cross-border data flows. *CIGI Papers,* 197. https://www.cigionline.org/static/documents/documents/paper%20no.197_0.pdf

Akbari, A. (2026). *Iran's case should put an end to illusions about digital sovereignty.* Tech Policy Press. https://www.techpolicy.press/irans-case-should-put-an-end-to-illusions-about-digital-sovereignty/

Ackoff, R. L. (1989). From data to wisdom. *Journal of Applied Systems Analysis, 16,* 3–9.

Allison, K., Benson, E., & Rugova, V. (2025). *Fortress America and the future of the global tech stack.* Minerva Technology Futures. https://minervapolicy.com/wp-content/uploads/2025/05/Minerva_2025_Fortress-America_report.pdf

Azmeh, S., Foster, C., & Abd Rabih, A. (2021). *The rise of the data economy and policy strategies for digital development* (Digital Pathways paper series No. 10). Blavatnik School of Government, University of Oxford. https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2021-02/data_economy_5feb21.pdf?utm_source=chatgpt.com

Banga, K., Macleod, J., & Mendez-Parra, M. (2021). *Digital trade provisions in the AfCFTA: What can we learn from South–South trade agreements?* (Supporting Economic Transformation [SET] working paper series). https://setodi2020.wpenginepowered.com/wp-content/uploads/2021/04/Digital-trade-provisions-in-the-AfCFTA.pdf

Basu, A., Hickok, E., & Chawla, A. S. (2019, March 19). *The localisation gambit: Unpacking policy measures for sovereign control of data in India.* Centre for Internet and Society. https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf

Belli, L., Britto Gaspar, W., & Jaswant, S. S. (2024). Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries. *Computer Law & Security Review, 54.* https://ssrn.com/abstract=4903196

Berger, C., Freihse, C., & Meyer zu Schwabedissen, O. (2024). *Effectively countering disinformation: Perspectives from every continent.* Bertelsmann Stiftung. https://www.bertelsmann-stiftung.de/en/publications/publication/did/effectively-countering-disinformation-perspectives-from-every-continent

Bradford, A. (2023). *Digital empires: The global battle to regulate technology.* Oxford University Press.

Burri, M. (2017). The governance of data and data flows in trade agreements: The pitfalls of legal adaptation. *UC Davis Law Review, 51,* 65–133. https://ssrn.com/abstract=3067973

Burri, M. (2019). Understanding the implications of big data and big data analytics for competition law: An attempt for a primer. In K. Mathis & A. Tor (Eds.) *New developments in competition law and economics.* Springer.

Burri, M. (2020). Trade in services regulation in the data-driven economy. *Trade, Law & Development, 12*(1). https://ssrn.com/abstract=3545103

Burri, M. & Polanco Lazo, R. (2019). Digital trade provisions in preferential trade agreements: Introducing a new dataset. *Journal of International Economic Law, 23*(1), 1–34. https://ssrn.com/abstract=3482470

Burri, M. & Chander, A. (2023). What are digital trade and digital trade law? *American Journal of International Law Unbound,* 117.

Burri, M. & Callo-Müller, M.V. (2025). *TAPED: Trade agreement provisions on electronic commerce and data.* https://unilu.ch/taped

Burri, M. & Kugler, K. (2024). Regulatory autonomy in digital trade agreements. *Journal of International Economic Law, 00,* 1–27. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4943323

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis.* Lynne Rienner Publishers.

Cai, K. G. (2010). *The politics of economic regionalism: Explaining regional economic integration in East Asia.* Palgrave Macmillan.

Callo-Müller, M.V. (2025). *Data protection provisions in PTAs. Training module on digital trade for Diplo Foundation and the Commonwealth Small States Office.*

Carrière-Swallow, Y., & Haksar, V. (2019). *The economics and implications of data: An integrated perspective.* International Monetary Fund. https://www.imf.org/-/media/Files/Publications/DP/2019/English/TEIDEA.ashx

Casalini, F. & López González, J. (2019). *Trade and cross-border data flows* (OECD trade policy papers no. 220). OECD Publishing. http://dx.doi.org/10.1787/b2023a47-en

Casillas, J. (2023). Bias and discrimination in machine decision-making systems. In Francisco Lara & Jan Deckers (Eds.) *Ethics of artificial intelligence.* Springer Nature.

Chander, A. (2022). Trump v. TikTok. *Vanderbilt Journal of Transnational Law, 55*(5).

Chander, A., & Sun, H. (Eds.). (2023). *From the digital Silk Road to the return of the state.* Oxford University Press.

Chen, Q. (2022). *China wants to put data to work as an economic resource—but how?* DigiChina. https://digichina.stanford.edu/work/china-wants-to-put-data-to-work-as-an-economic-resource-but-how/

Ciuriak, D. (2022a). *The geopolitics of the data-driven economy.* Centre for International Governance Innovation, C.D. Howe Institute, Asia Pacific Foundation of Canada, & Balsillie School of International Affairs. https://ssrn.com/abstract=3770470

Ciuriak, D. (2022b). *Unfree flow with no trust: The implications of geoeconomics and geopolitics for data and digital trade.* Centre for International Governance Innovation. https://www.cigionline.org/articles/unfree-flow-with-no-trust-the-implications-of-geoeconomics-and-geopolitics-for-data-and-digital-trade/

Cory, N. (2021). *How 'Schrems II' has accelerated Europe's slide toward a de facto data localization regime.* Information Technology and Innovation Foundation. https://itif.org/publications/2021/07/08/how-schrems-ii-has-accelerated-europes-slide-toward-de-facto-data/

Couldry, N., & Mejias, U. A. (2018). Data colonialism: Rethinking big data's relation to the contemporary subject. *Television & New Media, 20*(4). https://doi.org/10.1177/1527476418796632

Daskal, J. (2016). Law enforcement access to data across borders: The evolving security and rights issues. *Journal of National Security Law and Policy, 473.* https://nationalsecurity.law.georgetown.edu/journal/2016/09/06/law-enforcement-access-data-across-borders-evolving-security-rights-issues/

Eisentrout, S. (2025). It's time to trust the Global South. *Foreign Policy.* https://foreignpolicy.com/2025/11/20/global-south-united-states-europe-global-leadership-multilateral-cooperation/

European Commission. (2023). *Joint communication to the European Parliament, to the European Council and the Council on "European Economic Security Strategy" Brussels, 20.6.2023 JOIN (2023) 20 final.* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023JC0020

European Commission. (2025). *Joint Communication to the European Parliament and the Council. Strengthening EU Economic Security. Brussels, 3.12.2025. JOIN (2025) 977 final.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025JC0977

Evenett, S. & Fritz, J. (2023). *Emergent digital fragmentation: The perils of unilateralism.* Joint Report of the Digital Policy Alert and Global Trade Alert. https://globaltradealert.org/reports/a-joint-report

Farboodi, M., & Veldkamp, L. (2021). *A growth model of the data economy* (Working paper 28427). National Bureau of Economic Research. https://www.nber.org/system/files/working_papers/w28427/w28427.pdf

Ferencz, J., López-González, J., & Oliván García, I. (2022). *Artificial intelligence and international trade: Some preliminary implications* (OECD trade policy paper no. 260). https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/04/artificial-intelligence-and-international-trade_9034b5f2/13212d3e-en.pdf

Foster, C., & Azmeh, S. (2020). Latecomer economies and national digital policy: An industrial policy perspective. *The Journal of Development Studies, 56*(7). https://www.tandfonline.com/doi/full/10.1080/00220388.2019.1677886

Fritz, J. & Giardini, T. (2023). *Data governance regulation in the G20.* Digital Policy Alert. https://digitalpolicyalert.org/report/fragmentation-risk-in-g20-data-governance-regulation

Gao, H. (2018). Digital or trade? The contrasting approaches of China and the US to digital trade. *Journal of International Economic Law, 21*(2), 297–321

Ghiretti, F. (2025). The return of economic security. *Internationale Politik Quarterly, 4.* https://ip-quarterly.com/en/return-economic-statecraft

Giovani, C. D., Ferencz, J., & López-González, J. (2023). *The nature, evolution and potential implications of data localisation measures* (OECD trade policy paper No. 278). https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/11/the-nature-evolution-and-potential-implications-of-data-localisation-measures_249df37e/179f718a-en.pdf

Guglya, L., & Maciel, M. (2020). *Addressing the digital divide in the Joint Statement Initiative on e-commerce: From enabling issues to data and source code provisions.* International Institute for Sustainable Development & CUTS International. https://www.iisd.org/system/files/2021-01/digital-divide-e-commerce-en.pdf

Gurumurthy, A. (2026, January). *Why a cross-track approach is necessary to steer the work of the CSTD Working Group on Data Governance.* IT for Change. https://itforchange.net/sites/default/files/add/CSTD%20inputs-ITfC-Jan2026.pdf

Henke, N., Libarikian, A., & Wiseman, B. (2016, February). *Straight talk about big data.* McKinsey Quarterly. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/straight-talk-about-big-data

International Monetary Fund, Organisation for Economic Co-operation and Development, United Nations, & World Trade Organization. (2023). *Handbook on measuring digital* trade (Second edition). https://www.wto.org/english/res_e/publications_e/digital_trade_2023_e.htm

Internet Society. (2019). *Internet society global internet report 2019: Consolidation in the internet economy.* https://www.internetsociety.org/wp-content/uploads/2022/12/2019-Internet-Society-Global-Internet-Report-Consolidation-in-the-Internet-Economy.pdf

Ismail, Y. (2021). *Cooperation capacity building, and implementation considerations of developing countries in the E-Commerce Joint Statement Initiative: Status and the way forward.* International Institute for Sustainable Development. https://www.iisd.org/publications/report/developing-countries-in-e-commerce-joint-statement-initiative

Kaas H. W. & Fleming T. (2014). *Bill Ford charts a course for the future.* McKinsey Quarterly. https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/bill-ford-charts-a-course-for-the-future

Kassa, W. (2025). Regionalization of global trade: A new order in the making. *Global Policy, 16*(4). https://onlinelibrary.wiley.com/doi/abs/10.1111/1758-5899.70033?campaign=wolearlyview

Kruse, L. & Grafenstein, M. V. (2025). Proprietary data, open data, data commons: Who owns the data? How to best reconcile conflicting interests in exploiting the value of data and protecting against its risks. *Computer Law & Security Review, 59.*

Kugler, K. (2022). *The impact of data localisation laws on trade in Africa* (Policy brief 8). Mandela Institute, School of Law, University of The Witwatersrand. https://www.wits.ac.za/media/wits-university/faculties-and-schools/commerce-law-and-management/research-entities/mandela-institute/documents/research-publications/PB%2008%20Data%20localisation%20laws%20and%20trade.pdf

Larsson, S. (2021). Putting trust into antitrust? Competition policy and data-driven platforms. *European Journal of Communication, 36*(4).

López González, J., Casalini, F., & Porras, J. (2022). *A preliminary mapping of data localisation measures* (OECD trade policy papers no. 262). OECD Publishing.

Maciel, M. (2023). *The renaissance of industrial policy and its articulation with data governance.* International Institute for Sustainable Development Trade Policy Review. https://www.iisd.org/articles/policy-analysis/industrial-policy-data-governance

Maciel, M., Morosini, F., & Tasquetto, L. (upcoming). Digital trade without development? Brazil's turn to industrial policy and competition law. *Journal of International Economic Law.*

Manak, I. (2025). *Repositioning the debate on subsidies and industrial policy.* Council on Foreign Relations. https://www.cfr.org/articles/repositioning-debate-subsidies-and-industrial-policy

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think.* Hachette.

Mejias, U. A., & Couldry, N. (2019). Datafication. *Internet Policy Review, 8*(4). https://policyreview.info/concepts/datafication

Merriam-Webster. (n.d.). Data. In *Merriam-Webster.com Dictionary.* https://www.merriam-webster.com/dictionary/data.

Mishra, N. (2024). *International trade law and global data governance: Aligning perspectives and practices.* Hart Publishing.

Mishra, N. (2025). Cybersecurity and international trade: Understanding the policy landscape. *(Building blocks of digital trade regulation series No. 2)*. International Institute for Sustainable Development. https://www.iisd.org/system/files/2025-08/cybersecurity-international-trade-policy.pdf

Morosini, F., Tasquetto, L., & Maciel, M. (2024). *Navigating the digital divide: Challenges and strategies for Latin American countries in e-commerce and data governance regulation* (LAPEG paper no. 1). Center for the Advancement of the Rule of Law in the Americas (CAROLA) at the Georgetown University Law Center. https://www.law.georgetown.edu/carola/wp-content/uploads/sites/29/2024/11/2024-LAPEG_1_Policy-Brief-Digital-Trade.pdf

Okano-Heijmans, M., Gomes, A., & Kono, D. (2023). *Strengthening digital economic security in Europe: Promote, shape, regulate and protect, please!* Clingendael Report. https://www.clingendael.org/sites/default/files/2023-10/Report_Strengthening_digital_economic_security_in_Europe.pdf

Organisation for Economic Co-operation and Development. (2019a). *Vectors of digital transformation* (OECD digital economy papers, no. 273). https://www.oecd.org/en/publications/vectors-of-digital-transformation_5ade2bba-en.html

Organisation for Economic Co-operation and Development. (2019b). *Enhancing access to and sharing of data: Reconciling risks and benefits for data re-use across societies.* https://read.oecd-ilibrary.org/science-and-technology/enhancing-access-to-and-sharing-of-data_276aaca8-en#page3

Organisation for Economic Co-operation and Development. (2022). *Fostering cross-border data flows with trust* (OECD digital economy papers, no. 343). https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/12/fostering-cross-border-data-flows-with-trust_617f8e3f/139b32ad-en.pdf

Organisation for Economic Co-operation and Development & World Trade Organization. (2025). *Economic implications of data regulation: Balancing openness and trust.* OECD Publishing. https://www.oecd.org/en/publications/economic-implications-of-data-regulation_aa285504-en.html

Omdia. (2025). *Global cloud infrastructure spending rose 21% in Q1 2025, 12 June.* https://omdia.tech.informa.com/pr/2025/jun/global-cloud-infrastructure-spending-rose-21percent-in-q1-2025

Paterson, J. M., Chang, S., Cheong, M., Culnane, C., Dreyfus, S., McKay, D. (2021). The hidden harms of targeted advertising by algorithm and interventions from the Consumer Protection toolkit, *International Journal on Consumer Law and Practice, 9,* Article 1. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3993496

Potluri, S. R., Sridar, V., & Rao, S. (2020). Effects of data localization on digital trade: An agent-based modeling approach, *Telecommunications Policy, 44*(9). https://doi.org/10.1016/j.telpol.2020.102022

Rikap, C. (2022). *Big tech: Not only market but also knowledge and information gatekeepers.* Institute for New Economic Thinking. https://www.ineteconomics.org/perspectives/blog/big-tech-not-only-market-but-also-knowledge-and-information-gatekeepers

Rowley, J. (2007). The wisdom hierarchy: representations of the DIKW hierarchy. *Journal of Information Science,* 33.

Schmitt, M. N. & Vihul, L. (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations.* Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence. Cambridge University Press. https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/2017-Tallinn-Manual-2.0.pdf

Soprana, M. (2021). The digital economy partnership agreement (DEPA): Assessing the significance of the new trade agreement on the block. *Trade, Law and Development, XIII*(1).

Spiezia, V. & Tscheke, J. (2020). *International agreements on cross-border data flows and international trade: A statistical analysis* (OECD science, technology and industry working papers 2020/09). https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/10/international-agreements-on-cross-border-data-flows-and-international-trade_3f86a429/b9be6cbf-en.pdf

Statista. (2025). *Big data statistics and facts.* https://www.statista.com/chart/17727/global-data-creation-forecasts/?utm_source=chatgpt.com

Steil, B., & Harding, E. (2024). *Soaring abuse of "national security" exceptions has wrecked the multilateral trading system.* Council on Foreign Relations. https://www.cfr.org/blog/soaring-abuse-national-security-exceptions-has-wrecked-multilateral-trading-system

Stubb, A. (2025). *The West's last chance: How to build a new global order before it's too late*. Foreign Affairs. https://www.foreignaffairs.com/united-states/wests-last-chance

Sukumar A. & Basu, A. (2025). The China gambit: Geoeconomics and the US' turn to informal data governance initiatives. *The Geopolitics of Transnational Data Governance, 13.* https://www.cogitatiopress.com/politicsandgovernance/article/view/10512

Sucker, F. (2025). *The AfCFTA protocol on digital trade.* Social Science Research Network. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5386851

Tozzi, D., & Marki, A. (2025). *Redata pode diminuir deficit na conta de servicos e aliviar as contas externas.* Broadcast. https://www.broadcast.com.br/ultimas-noticias/especial-redata-pode-diminuir-deficit-na-balanca-de-servicos-e-aliviar-contas-externas/

United Nations General Assembly. (2025). *Default rules for data provision contracts (third revision) United Nations Commission on International Trade Law Working Group IV (Electronic Commerce) Sixty-eighth session New York, 24–28 March 2025* (A/CN.9/WG.IV/WP.188) https://docs.un.org/en/A/CN.9/WG.IV/WP.188

United Nations Conference on Trade and Development. (2014). *Studies in technology transfer: Selected cases from Argentina, China, South Africa and Taiwan Province of China* (UNCTAD Current studies on Science, Technology and Innovation, No. 7). https://unctad.org/publication/studies-technology-transfer-selected-cases-argentina-china-south-africa-and-taiwan

United Nations Trade and Development. (2021). *Cross-border data flows and development: For whom the data flow* (Digital economy report 2021). https://unctad.org/publication/digital-economy-report-2021

United Nations Trade and Development. (2024). *Data for development.* https://unctad.org/system/files/official-document/dtl-tikd2024d2_en.pdf?utm_source=chatgpt.com

United Nations Trade and Development. (2025). *Digital economy and technology Data insights.* https://unctadstat.unctad.org/insights/theme/119

United States Trade Representative. (2023). *USTR Statement on WTO E-Commerce Negotiations.* https://ustr.gov/about-us/policy-offices/press-office/press-releases/2023/october/ustr-statement-wto-e-commerce-negotiations

Weinhardt, C., & de Ville, F. (2024). The geoeconomic turn in EU trade and investment policy: Implications for developing countries. *Politics and Governance, 12*(1). https://www.cogitatiopress.com/politicsandgovernance/article/view/8217

Whittaker, M. (2023). Building muscle in infrastructure. In C. Cath (Ed.), *Eaten by the internet.* Meatspace Press.

Willemyns, I. (2021). *Digital services in international trade law.* Cambridge University Press.

World Bank. (2020). *Poverty and shared prosperity 2020: Reversals of fortune*. https://openknowledge.worldbank.org/bitstream/handle/10986/34496/9781464816024.pdf

World Economic Forum. (2021). *The global risks report 2021.* https://www.weforum.org/reports/the-global-risks-report-2021

World Trade Organization. (2023). *World Trade Report—Re-globalization for a secure, inclusive and sustainable future.* https://www.wto.org/english/res_e/publications_e/wtr23_e.htm

Yap, C. W. (2024). *The age of data.* Hinrich Foundation. https://www.hinrichfoundation.com/research/infographics/age-of-data

Zhang, S. & Gao, H. (2025). Bridging the Great Wall: China's evolving cross-border data flow policies and implications for global data governance. *Computer Law and Security Review, 59*, Article 106208. https://doi.org/10.1016/j.clsr.2025.106208

Published by the International Institute for Sustainable Development

Head Office

111 Lombard Avenue, Suite 325
Winnipeg, Manitoba
Canada R3B 0T4

IISD

iisd.org