INTERNATIONAL INVESTMENT AGREEMENTS AND THE DIGITAL ECONOMY

April 25, 2026
Doha, Qatar

Submitted by:

Muna Nasser Al-Kaabi
Noora Abdulrahman Al-Thani
Kulsoom Khan
Divya Jyoti Yadav
Marwan Omer Dahab Fadl
Mariia Khorolska

Prepared for:
United Nations Conference on Trade and Development (UNCTAD), International Investment Agreements Section

TradeLab output is prepared on a pro bono basis by students as a pedagogical exercise. It is not professional legal advice and in no way establishes a client-attorney relationship.

Executive Summary 1

1. Introduction **6**
2. Scope and Methodology **9**
2.1. Scope 9
2.2. Methodology 10
3. Mapping Digital Economy Provisions in IIAs **12**
3.1. Scope of the mapping 12
3.1.1 Overview by Country 12
3.1.2 Distribution by Treaty Type 13
3.1.3 Temporal Distribution 14
3.1.4 Geographic Scope 15
3.2. Presence of Digital-Specific Provisions 15
3.2.1 Dedicated Digital Chapters 15
3.2.2 Digital Provisions Embedded in Investment Chapters 16
3.2.3 Country-Level Patterns and Regional Observations 17
3.3. Data Governance and Performance Requirements 18
3.3.1 Cross-Border Data Flow Commitments 19
3.3.2 Data Localization Restrictions 20
3.3.3 Right to Regulate Clauses Relating to Digital Policy 20
4. Domestic Digital Policy and Treaty Interaction **21**
4.1. Armenia 22
A. Domestic Digital Policies *22*
B. Treaty Practice in the Digital Sphere *24*
C. Domestic law-IIA Interaction *26*
4.2. Brazil 28
A. Domestic Digital Policy Framework *28*
B. Treaty Practice in the Digital Sphere *30*
C. Domestic Law – IIA Interaction *34*
4.3. Colombia 35
A. Domestic Digital Policy Framework *35*
B. Treaty Practice in the Digital Sphere *37*
C. Domestic Law - IIA Interaction *39*
4.4. Costa Rica 40
A. Domestic Digital Policies *41*
B. Treaty Practice in the Digital Sphere *42*

C. Domestic Law – IIA Interaction *44*
4.5. Kenya 45
A. Domestic Digital Policy Framework *45*
B. Treaty Practice in Digital Sphere 48
C. Domestic Law - IIA Interaction 51
4.6. Mexico 53
A. Domestic Digital Policies *53*
B. Mexico's Treaty Practice in the Digital Sphere *54*
C. Domestic Law – IIA Interaction *55*
4.7. Nigeria 56
A. Domestic Digital Policy Framework *56*
B. Treaty Practice in the Digital Sphere *58*
C. Domestic Law - IIA Interaction 60
4.8. Pakistan 62
A. Domestic Digital Policies *62*
B. Treaty Practice in the Digital Sphere *63*
C. Domestic Law – IIA Interaction *65*
4.9. Peru 66
A. Domestic Digital Policies *66*
B. Treaty Practice in the Digital Sphere *68*
C. Domestic Law - IIA Interaction *72*
4.10. Rwanda 74
A. Domestic Digital Policies *74*
B. Treaty Practice in the Digital Sphere *77*
C. Domestic law - IIA Interaction *82*
4.11. Saudi Arabia 83
A. Domestic Digital Policies *83*
B. Treaty Practice in the Digital Sphere *86*
C. Domestic Law - IIA Interaction *89*
4.12. Singapore 90
A. Domestic Digital Policy Framework *90*
B. Treaty Practice in the Digital Sphere *93*
C. Domestic Law - IIA Interaction *95*
4.13. South Africa 97

A. Domestic Digital Policy Framework *97*
B. Treaty Practice in the Digital Sphere *99*
C. Domestic Law - IIA Interaction 100
4.14. Thailand 103
A. Domestic Digital Policies *103*
B. Thailand's Treaty Practice in the Digital Sphere *104*
C. Domestic Law – IIA Interaction *106*
4.15. Türkiye 106
A. Domestic Digital Policy Framework 107
B. Treaty Practice in the Digital Sphere 108
C. Domestic Law – IIA Interaction 110
5. Development Dimension 111
5.1. Defining Development-Oriented Provisions in IIAs 111
5.2. Empirical Findings 113
5.3. The Direction of Influence: Domestic Policy and Treaty Interaction 117
5.4. Answering the Research Questions 119
5.5. Implication for Policymakers 120
6. Conclusion 122
Annex 124

Executive Summary

This report examines how international investment agreements ('IIAs') respond to the digital economy, with particular focus on whether they promote or support development-oriented outcomes. It is based on a mapping of 77 IIAs across 15 countries: Armenia, Brazil, Colombia, Costa Rica, Kenya, Mexico, Nigeria, Pakistan, Peru, Rwanda, Saudi Arabia, Singapore, South Africa, Thailand, and Türkiye. The report draws on a broad understanding of IIAs, including BITs, FTAs with investment provisions, CEPAs, DEAs, DTAs, EU digital partnerships, and regional frameworks, as relevant.

The report's starting point is that the global economy has changed faster than international investment law. Investment is increasingly directed toward digital sectors, including data centers, fintech, artificial intelligence, e-commerce, cloud services, digital infrastructure, and platform-based business models. However, most IIAs were drafted for what the report describes as a 'traditional economy', which is an economy centered on physical assets, traditional infrastructure, manufacturing, and extractive industries. Therefore, there is a growing gap between contemporary digital investment and the treaty frameworks that govern it, with the widest gaps governing the more liberal aspects of digital investment, such as cross-border data flows and the protection of source codes.

The report finds that digital economy provisions are increasingly present in newer agreements, but their distribution remains uneven. Of the 77 agreements studied, 31 include a dedicated digital chapter, while 11 include partial digital chapters. This means that just over half of the agreements contain some form of dedicated or partial digital chapter. However, 35 agreements contain no dedicated digital chapter, and the distribution is not equal across the 15 countries, as the presence of such chapters is also highly concentrated. Singapore accounts for a large share of agreements with dedicated or partial digital chapters, which reflects the country's active role in exporting its domestic digital governance model through treaty practice and positioning itself as a leader among developing countries.

The report also finds that digital provisions are often not located in investment chapters. Instead, they are frequently placed in e-commerce, digital trade, cooperation, services, or general economic

partnership chapters. This is an important consideration because provisions outside core investment agreements are often less enforceable, less aligned with investor obligations, and less capable of directing investment toward development outcomes. Due to the frequency of soft-law recommendations, many agreements do not significantly reshape investment law.

Data governance is also examined in the dataset. The dataset contains right-to-regulate terms, source code protections, data localization limitations, and cross-border data flow regulations. However, these provisions are not evenly distributed, as only a few agreements from digitally advanced treaty-makers, such as Singapore and certain Latin American countries influenced by CPTPP or USMCA-style drafting, contain such liberalizing provisions. In particular, binding data flow commitments are highly concentrated in agreements with Singapore, accounting for 16 of the 26 containing such provisions(61.5%). Costa Rica (3), Brazil (2), Mexico (2), Peru (2), and Thailand (2) all provide more examples of significant data flow promises. This division shows that free flow of data provision is found in the Asia-Pacific and in several Latin American Treaty practice, but is absent from the IIAs of African and Central Asian parties included in the database.On the other hand, countries in Africa and Central Asia, as well as those that rely on traditional BIT-style agreements, tend to include only limited or no data-governance disciplines.

The country case studies in the paper demonstrate the various ways in which treaty practice and domestic digital policy interact. Treaty obligations are preceded and made possible by domestic legislation in some nations. For instance, nations that already have frameworks for electronic transactions, cybersecurity rules, data protection laws, and digital strategies are better positioned to embrace aspects of digital treaties without requiring significant domestic transformation. This is evident in nations such as Brazil, Saudi Arabia, Rwanda, and Kenya, where domestic digital policy has evolved either before or concurrently with treaty engagement.

In other instances, domestic digital governance is impacted by treaty practice. The impact of external treaty models is evident in Mexico's digital treaty obligations, especially through the USMCA framework. Similarly, Thailand's treaty practice reflects regional and ASEAN-based approaches rather than a unique national model extended outward. Additionally, Armenia also exhibits the international-to-domestic type of influence, especially through the EU and EAEU frameworks.

The most striking example of domestic-to-international influence is Singapore. Its Smart Nation framework, Digital Economy Agreements, and domestic digital economy plan demonstrate how a nation with a developed digital governance model can project its regulatory preferences into international agreements. In contrast to many developing countries, which are better characterized as rule-takers rather than rule-makers in the practice of digital treaties, this is a very distinctive example.

The report's development dimension is its most important finding. Provisions focused on development are still few, inadequate, and inconsistent. According to the research, development-oriented measures include support for domestic capacity-building, technological advancement, digital infrastructure, equitable participation, SME inclusion, and regulatory competence, in addition to traditional investment protection and liberalization. The report concludes that such clauses remain uncommon when evaluated by this criterion. Only a small percentage of agreements have technology transfer clauses. Although they are more apparent, capacity-building and technical support programs are still scarce. Finally, the rarest development-oriented regulations concern SME and digital inclusion.

However, right-to-regulate clauses are far more prevalent. This implies that rather than being approached positively, progress is mainly tackled defensively. In other words, IIAs are more inclined to protect policy space than to actively require investment to contribute to digital development. This is important because policy space is both a requirement for states to have space for their own policies and a limit on how some digital provisions may apply. A treaty may safeguard a state's regulatory authority, but it won't advance technology transfer, infrastructure development, skill development, or equitable access to the digital economy.

Additionally, the research notes that when development-oriented clauses are included, they are typically phrased in a soft, best-endeavour language. For instance, phrases like "*the Parties shall endeavor to cooperate*" are frequently used. These kinds of clauses might be effective in expressing political intent, but they do not create funding commitments or enforceable obligations. Additionally, rather than being integrated into the agreement's primary investment regulations, development clauses are frequently included in cooperation chapters. As a result, development provisions have limited effects.

One of the most significant exceptions is the AfCFTA structure. By connecting investment, digital development, infrastructure, technology transfer, sustainable development, and regulatory policy space, it represents a more development-sensitive treaty structure. It is still unique, though, and does not reflect more general treaty practice. Similarly, agreements such as the UK-Singapore DEA and the Indonesia-UAE CEPA mention capacity-building, cooperation, inclusion, and SME participation, but these clauses are mostly programmatic.

Three research questions are answered in the report. First, digital economy provisions are unevenly present in modern IIAs. They are primarily found in more recent agreements, regional frameworks, and agreements involving treaty-makers with extensive digital capabilities. Second, there is an uneven link between IIA provisions and domestic frameworks. While some nations follow external treaty models, those with developed domestic digital frameworks are better positioned to set treaty regulations. Third, IIAs continue to marginalize digital development. Compared to liberalization or data-governance requirements, development provisions are less prevalent, less legally obligatory, and less integrated.

The report comes to the conclusion that, despite their growing regulation of the digital economy, IIAs remain ill-prepared to advance the objectives of digital development because they do not yet consistently direct digital investment toward inclusive development. The main advice for legislators is to create better digital provisions rather than just adding more. Future IIAs ought to incorporate greater operational development commitments and go beyond general cooperation language by identifying beneficiaries, mechanisms, institutional responsibilities, and implementation pathways.

Instead of limiting development-oriented measures to auxiliary cooperation sections, policymakers should incorporate them into the structure of investment chapters. Additionally, there should be a stronger link between investment activities and the Sustainable Development Goals ('SDGs'), including technology transfer, capacity building, infrastructure assistance, and SME inclusion. Prioritizing local digital capabilities is especially important for developing nations before entering into legally binding commitments in the digital economy. Robust domestic regulations on data protection, cybersecurity, e-commerce, digital identity, AI governance, infrastructure, and SME

digitalization enhance negotiating power and reduce the likelihood of becoming passive beneficiaries of external treaty models.

Overall, the report finds that the digital economy has entered international investment law, but digital development has not yet done so systematically. The next generation of IIAs should therefore move from digital liberalization toward digital development.

1. Introduction

The global economy has undergone a major structural transformation over the past two decades. The emergence and expansion of the digital economy mainly drove this restructuring. This transformation relates to the massive ecosystem of interrelated, intricate, and dynamic interactions between people and the built environment.[1] This revolution has been mainly paved by technologies such as Artificial Intelligence ('AI'), the Internet of Things ('IoT)', cloud computing, big data analytics, blockchain, and platform-based businesses.[2]

These transformations have had profound implications for international investment. In fact, foreign direct investment ('FDI'), which is traditionally associated with sectors such as manufacturing, extractive industries such as the various natural resources industries, and infrastructure, is now increasingly being directed towards the digital sector, which includes FDI directed at data centers, digital services, fintech, e-commerce, and platform-based businesses.[3] Furthermore, UN Trade and Development also evidenced that greenfield investments in digital sectors have expanded greatly since the early 2020s,[4] indicating increased interest in investments in the digital sphere.

However, growing interest in digital trade remains uneven across regions, widening the digital divide. Countries with advanced digital infrastructure, coherent regulatory frameworks, and strong data governance, such as Singapore and the European Union, have emerged as leading hubs for FDI in the digital economy. In contrast, many developing economies face structural barriers that limit or slow their participation, including inadequate infrastructure, fragmented regulations, skills gaps, and limited access to capital.[5] This unequal distribution raises important questions on the role of international economic law in either reinforcing or mitigating digital divides.

---

[1] United Nations Conference on Trade and Development, *Digital Economy Report 2024: Shaping an Environmentally Sustainable and Inclusive Digital Future* (UN 2024) 3–5

[2] Thomas Philbeck and Nicholas Davis, 'The Fourth Industrial Revolution: Shaping a New Era' (2018) 72(1) *Journal of International Affairs* 17, 20.

[3] United Nations Conference on Trade and Development, *World Investment Report 2024: Investment Facilitation and Digital Government* (UN 2024) 10–15

[4] UNCTAD, 'Global Investment in the Digital Economy Surges but Remains Uneven' (25 August 2025) https://unctad.org/news/global-investment-digital-economy-surges-remains-uneven accessed 13 April 2026.

[5] World Bank, *World Development Report 2021: Data for Better Lives* (2021) 168-171.

International investment agreements ('IIAs') were, for the most part, designed for a world that no longer exists. The bulk of the 2,856 Bilateral Investment Treaties ('BITs') currently recorded in the UNCTAD IIA Navigator were negotiated with traditional, capital-intensive investment in mind. They say very little about digital investment, data-driven business models, or the role investment might play in supporting digital development. The same is broadly true of Treaties with Investment Provisions ('TIPs') and many of the newer generation of instruments. The result of this is a widening gap between how investment actually works today and what treaty law provides for.

The legal consequences of this mismatch are concrete. Most IIA definitions of investment are asset-based and were not drafted with intangible digital assets in mind. Whether data, algorithms, software, or digital platforms qualify as protected investments under existing treaties remains genuinely contested. That definitional uncertainty compounds the broader problem that even where disputes arise from digital investment activity, the applicable treaty framework may offer limited guidance on coverage, let alone on the standards of treatment that should apply.

This fragmentation due to the traditional nature of IIAs is most evident in the realm of data as they were related to provisions in a 'traditional economy' which will be explored later. The governance of data, particularly cross-border data flows, data localization requirements, and data protection standards, has become a crucial determinant of investment decisions in digital sectors.[6] However, data issues are addressed in newer international agreements, with some agreements addressing aspects of the digital economy more directly and holistically. These international agreements include Digital Economy Agreements ('DEAs'), Digital Trade Agreements, and digitally focused chapters within Free Trade Agreements ('FTAs').

Some agreements have started to move in a different direction. Singapore's Digital Economy Agreements, the EU's Digital Partnerships and Digital Trade Agreements, and plurilateral frameworks such as the Indo-Pacific Economic Framework for Prosperity each include provisions touching on cross-border data flows, data localization, source code protection, and digital infrastructure. There have even been plurilateral discussions and soft agreements addressing the data issue, such as the WTO Joint Statement Initiative on Electronic Commerce ('JSI'), which

[6] OECD and WTO, *Economic Implications of Data Regulation: Balancing Openness and Trust* (OECD Publishing 2024) 9–10 https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/09/economic-implications-of-data-regulation_7a6a28ba/aa285504-en.pdf accessed 13 April 2026.

represents efforts to develop baseline multilateral rules governing digital trade (although the JSI remains largely a soft law and its integration into the WTO legal framework is still under dispute).[7] But coverage is uneven, enforceability varies widely, and the connection between these treaty commitments and the domestic digital policies of the countries involved has received little systematic attention. That unevenness is itself revealing. It points to a real and unresolved tension in international investment governance between pushing for regulatory openness on one hand and preserving domestic control over data, technology, and digital infrastructure on the other. For many states, both objectives matter, and existing treaty frameworks struggle to accommodate them simultaneously.

The way regional and international superpowers are tackling these issues is also affecting how countries work together on digital issues. The United States, the European Union, and China are all creating their own rules for the digital world in different ways. The US is working with a small group of countries on agreements like IPEF and making deals with individual countries on digital trade. The EU is creating its own set of rules and partnerships, based on its own unique way of regulating things. Lastly, China is making agreements with other countries and expanding its influence through initiatives such as the Digital Silk Road project. Therefore, all these different approaches aren't leading to a common set of rules. Instead, they're creating a complicated landscape that's hard for countries to navigate.

There is a further problem that has received even less attention. Development-oriented provisions in IIAs, those addressing digital inclusion, technology transfer, capacity-building, or support for smaller enterprises, are rare. Digital FDI remains heavily concentrated in a handful of wealthy and large emerging economies. The treaty architecture that could, in principle, help channel investment toward broader development goals has not kept up, and for developing countries trying to use IIAs as part of a wider digital industrial policy, this is a significant constraint.

This report, prepared for UNCTAD, directly addresses these questions. It pursues three connected objectives: The first is to map digital economy provisions across the IIA landscape, drawing on both the IIA Navigator and the newer generation of digital-specific agreements. The second is to

[7] WTO, 'Joint Statement Initiative on Electronic Commerce' https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm accessed 13 April 2026.

examine how domestic digital policy frameworks and IIA provisions interact, using 15 country case studies spanning different legal traditions and levels of development. The third is to assess how development considerations feature in these frameworks, and whether digital-economy-related IIA provisions are actually designed to support inclusive growth.

The report is structured as follows. Section 2 explains the methodology and scope of the mapping. Section 3 presents the mapping results and develops a typology of digital economy provisions across IIAs. Section 4 works through the domestic-treaty interaction for each of the fifteen case studies. Section 5 turns to the development dimension. Section 6 closes with policy recommendations for those negotiating and designing investment agreements in the digital age.

2. Scope and Methodology

2.1. Scope

This report analyzes IIAs involving 15 specific countries identified as developing countries in the United Nations Conference on Trade and Development ('UNCTAD') World Investment Report 2025.[8] The time period focused is the 2021 onwards, with exceptions and added extension for countries that had little or no IIAs in that time period, as digital provisions started becoming more common during this period. The analysis focuses not only on the international agreements themselves but also on domestic laws, policies, and guidelines within these fifteen countries in order to examine how domestic regulatory frameworks interact with and shape the international investment norms.

The report uses a broad definition of the IIAs, consistent with the UNCTAD IIA Navigator. It refers to a wide range of international agreements which includes BITs, such as Canada's Foreign Investment Promotion and Protection Agreements ('FIPAs'). It also covers FTAs and comprehensive economic partnership or cooperation agreements ('CEPAs' 'CECAs') that contain dedicated investment chapters. In addition, it includes DEAs, EU Digital Partnerships, and Digital

[8] United Nations Trade and Development (UNCTAD), 'World Investment Report 2025: International Investment in the Digital Economy' (United Nations Research Institute for Social Development 2025) <https://unctad.org/system/files/official-document/wir2025_en.pdf>.

Trade Agreements ('DTAs'). However, memoranda of understanding ('MoUs') and other solely soft-law agreements associated with the Digital Silk Road are excluded from the main mapping exercise.

The domestic laws and regulations are also analysed beyond the international agreements. Each selected country's digital economy legal framework is analyzed to assess how domestic provisions support, conflict with, or complement the IIAs. By mapping these domestic laws, the report identifies the degree to which national policies influence the treaty practice and international investment and how the opposite may as well be true by IIAs influencing domestic policies and law. Therefore, this report analyzes the extent to which domestic policies and a country's treaty practice interact, whether they shape, influence, or only contain gaps with no discernible interaction between the two. The report also contains a digital repository of all IIAs discussed per country linked in the Annex which is used for country level analysis and wider level analysis and statistics for mapping.

2.2. Methodology

The methodological framework combines qualitative and quantitative approaches. Three databases were primarily used: The UNCTAD IIA Navigator acts as a baseline for treaty identification.[9] The Trade Agreements Provisions on Electronic-commerce and Data ('TAPED') database offers a classification of digital provisions in trade and investment agreements.[10] The Industrial Policy and Digital Development ('IPDD') database and its country profiles by HBKU maps the domestic digital policy context.[11] The databases aided in enabling comparison of national regulatory choices against IIA commitments. However, since some agreements were drafted in languages other than English, AI translation tools were used for interpretation.

The analytical framework adopts a two-cluster approach to digital trade and investment provisions. The first cluster comprises rules that facilitate digital trade by addressing discrete issues, including

[9] 'International Investment Agreements Navigator | UNCTAD Investment Policy Hub' <https://investmentpolicy.unctad.org/international-investment-agreements> accessed 24 April 2026.
[10] Universität Luzern, 'TAPED' (*University of Lucerne*) <https://www.unilu.ch/en/faculties/faculty-of-law/professorships/burri-mira/research/taped/> accessed 24 April 2026.
[11] Georgios Dimitropoulos and others, 'IPDD Database | Hamad Bin Khalifa University' <https://www.hbku.edu.qa/en/cl/ipdd/database> accessed 24 April 2026.

paperless trading, electronic contracts, and electronic authentication, while also promoting business and consumer trust. The second cluster relates to data governance, particularly cross-border data flows and broader data economy considerations, including regulatory, developmental, and security dimensions.[12] It indicates that a substantial number of preferential trade agreements contain facilitation-oriented provisions, with some convergence observable in treaty language within this cluster. In contrast, data governance provisions remain more heterogeneous and contested across jurisdictions. This two-cluster typology guided both the selection of relevant provisions and their subsequent coding and categorization.

For the analysis, firstly agreements with digital provisions are selected. A provision is treated as investment-relevant if it: (i) directly regulates or facilitates digital-economy-related investment; (ii) imposes obligations on investors or states with respect to data, software, or digital assets; (iii) governs the conditions under which states may adopt measures affecting digital investment in pursuit of public policy objectives; or (iv) includes cooperation, promotional, or development-oriented commitments expressly referencing the digital economy or technology transfer.

Secondly, these provisions are compared against the domestic regulatory environments. This comparison is facilitated by a structured Excel database,[13] where the treaties are identified and the domestic-treaty interaction is also checked. Each entry is coded based on the presence and interaction of digital obligations, enabling cross-country comparison. Quantitative coding allows the frequency and type of digital provisions to be measured and compared. The qualitative analysis identifies patterns of alignment or divergence between domestic and international frameworks.

Finally, since a full-text review of every digital provision within all agreements examined was not feasible, the report employs a structured keyword search strategy. Search terms were organized into two categories, as set out in the table below:

Category	**Search Terms**

[12] Mira Burri, 'Digital Trade: New Design Elements in Preferential Trade Agreements' in Kathleen Claussen, Manfred Elsig and Rodrigo Polanco (eds), *The Concept Design of a Twenty-First Century Preferential Trade Agreement* (1st edn, Cambridge University Press 2025) <https://doi.org/10.1017/9781009484640.008> accessed 24 April 2026.

[13] See Annex.

Broad-scope terms	digital, data, development, investment, electronic, cyber, ICT, e-commerce, technology, digital infrastructure
Narrow-scope terms	data localization, source code, cross-border data flows, data center, cloud, technology transfer, digital development, capacity building

Table 2.2. Keyword Classification for Agreement Screening and Provision Identification

The broad-scope terms were applied during the initial screening phase to identify potentially relevant agreements. Narrow-scope terms were subsequently used to isolate provisions directly relevant to the report's analytical focus, with particular attention to the data governance category identified above.

3. Mapping Digital Economy Provisions in IIAs

3.1. Scope of the mapping

The digital repository includes IIAs of 15 countries between 2021 and 2026 (linked in Annex 1). Certain countries did not enter into many IIAs during this short time period, and therefore, there are a few exceptions to the five-year rule. The repository includes information that was sourced from the UNCTAD IIA Navigator, Trade Agreement Provisions on Electronic-commerce and Data ('TAPED)', and original treaty documents. In this report, we compare the treaties entered into by the 15 states with their domestic laws to examine any possible relationships between the two and whether one influences the other.

3.1.1 Overview by Country

This report covers 15 countries: Armenia, Brazil, Colombia, Costa Rica, Kenya, Mexico, Nigeria, Pakistan, Peru, Rwanda, Saudi Arabia, Singapore, South Africa, Thailand, and Turkey. Singapore accounts for the majority of the data, with 29 IIAs, demonstrating how active and advanced its treaty processes are. Mexico and Peru each have 7 agreements, while Thailand has 8 agreements. Some nations, such as Rwanda, Nigeria, and Colombia, appear to have just one or two agreements, implying that they are more selective or are only starting to engage in treaty negotiations that involve digital trade provisions.

Country	IIAs Identified	% of Dataset	Notable Characteristic
Singapore	29	37.7%	Most active; inclusive digital engagement
Thailand	8	10.4%	Mix of FTAs and DEAs with emerging digital provisions
Mexico	7	9.1%	Strong FTA tradition; modernised USMCA-influenced provisions
Peru	7	9.1%	Increasingly proactive digital treaty drafting
Kenya	6	7.8%	AfCFTA and EAC agreements; limited standalone digital
Costa Rica	5	6.5%	Growing digital chapter inclusion in recent FTAs
Armenia	4	5.2%	EU-aligned; EAEU digital framework (secondary law)
Brazil	3	3.9%	Emerging digital economy agreements (DEAs)
Pakistan	2	2.6%	Traditional BIT architecture; minimal digital content
Rwanda	1	1.3%	Single AfCFTA-linked agreement; developing digital engagement
Nigeria	1	1.3%	Singapore BIT; no standalone digital provisions
Colombia	1	1.3%	FTA with digital chapter
Turkey	1	1.3%	FTA with dedicated digital chapter
South Africa	1	1.3%	UK EPA; partial digital chapter

Table 3.1 - Distribution of IIAs by Country

3.1.2 Distribution by Treaty Type

The dataset includes a wide range of treaty types, demonstrating how international investment law is growing increasingly complicated. The largest group, FTAs and Treaties with Investment Provisions in the FTA structure, accounts for approximately 39% of the dataset, with 30 agreements. BITs account for 20.8%, with 16 agreements, including older treaties and a few freshly signed ones.

DEAs, which are relatively recent, are featured five times (6.5%), the majority of which is tied to Singapore's treaty practice. The remaining 21% (16 agreements) are of different types, including plurilateral protocols, economic union treaties, and association agreements. In addition, DPA-EU agreements and CEPAs each include a modest number of agreements.

3.1.3 Temporal Distribution

The majority of the information focuses on recent treaty action. In fact, 46 out of 77 agreements, or more than 59% of them, were reached between 2020 and 2025. 2023 was the busiest year in the dataset, with 17 new agreements in that year. In addition to initiatives in Asia, Latin America, and Africa to modernize their frameworks for international investment agreements, this recent emphasis demonstrates how the digital economy has emerged as a major focus for treaty-making following COVID-19. With a total of 15 agreements, there was also significant activity in 2018 and 2019. Major plurilateral agreements like the CPTPP began to take shape during this time, while Singapore's bilateral digital agreements began to roll out rapidly.

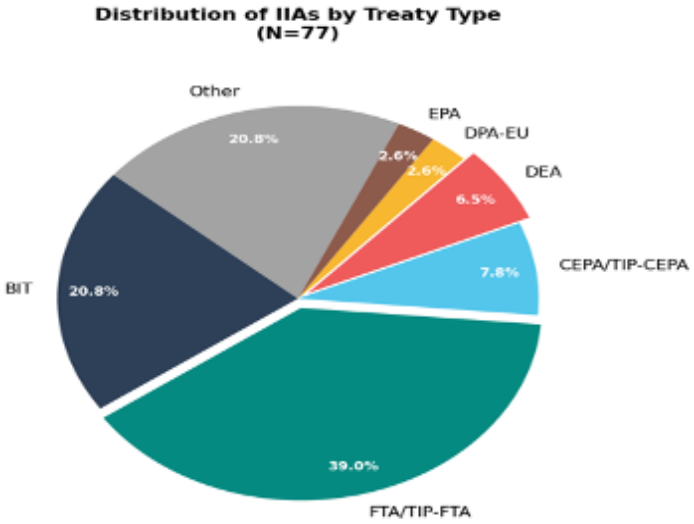


Figure 3.1: Distribution of IIAs by Treaty Type

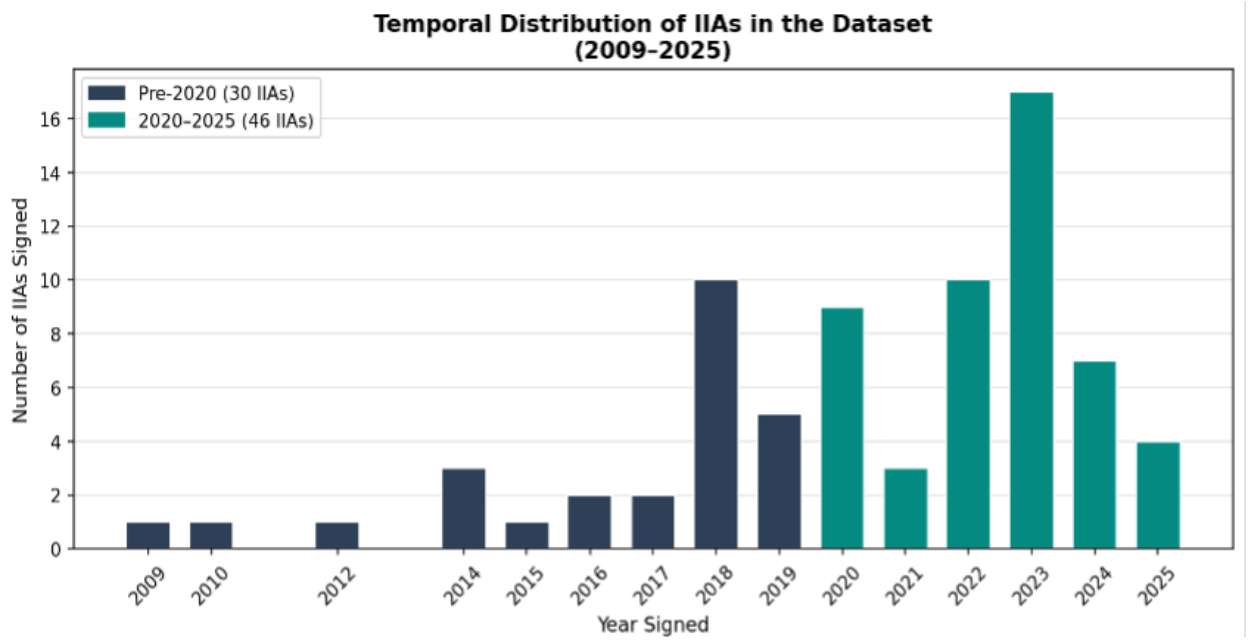


Figure 3.2 - Temporal Distribution of IIAs Signed (2009-2025)

3.1.4 Geographic Scope

Looking at geographic scope, BITs account for about 43% of all agreements when you combine different types. Preferential Trade Agreements make up around 25%. Regional agreements, like the EAEU Treaty and AfCFTA protocols, account for about 9%, while intercontinental frameworks such as EU-based deals cover roughly 8%. This shows that bilateral negotiations are still the main method for managing digital investment, although plurilateral and regional approaches are starting to become more common, especially in Southeast Asia and Sub-Saharan Africa, as is evidenced by literature on the topic.[14]

3.2. Presence of Digital-Specific Provisions

The core idea of mapping is to determine the frequency and kind of digital economy provisions that are present in the sampled IIAs. In this section, a distinction is made between two types of digital engagement strategies: incorporating digital-related provisions into more general investment chapters (usually as additional protections or carve-outs) and creating dedicated digital chapters, which are separate treaty sections created especially to regulate digital trade and investment. These two modes can coexist inside a single agreements and are not mutually incompatible, as is also understood from the TAPED dataset and the subsequent research that resulted from the dataset.[15]

3.2.1 Dedicated Digital Chapters

Of the 77 agreements studied, 31 (40.3%) include a dedicated digital chapter, which is a single treaty section that addresses digital trade, electronic commerce, or the digital economy. Another 11 agreements (14.3%) have incomplete digital chapters, which are agreements with digital provisions organized in a named section but restricted in scope. This suggests that about 54.5% of

[14] Woubet Kassa, 'Regionalization of Global Trade: A New Order in the Making' (2025) *Global Policy* 773, 774.

[15] Mira Burri, María Vásquez Callo-Müller and Kholofelo Kugler, *TAPED: Trade Agreements Provisions on Electronic Commerce and Data – Codebook* (2025) 3 https://www.unilu.ch/fileadmin/fakultaeten/rf/burri/TAPED/Codebook_TAPED_Burri_Vasquez_2025.pdf accessed 13 April 2026.

the sampled IIAs have some type of specific digital chapter architecture. In comparison, 35 agreements (45.5%) have no specific digital chapter.

The presence of dedicated digital chapters is highly concentrated among a small number of active parties. Singapore accounts for 21 of the 42 agreements featuring a dedicated or partial digital chapter (50%), followed by Peru (4), Costa Rica (3), Mexico (3), Thailand (3), and Brazil (3). For Singapore, dedicated digital chapters appear in agreements concluded under DEAs, TIP-FTA, and CEPA formats, while for Latin American partners, they tend to appear in FTAs that follow CPTPP-influenced templates. This concentration confirms that the digital chapter architecture, while increasingly common, remains most systematically deployed by a handful of digitally progressive economies

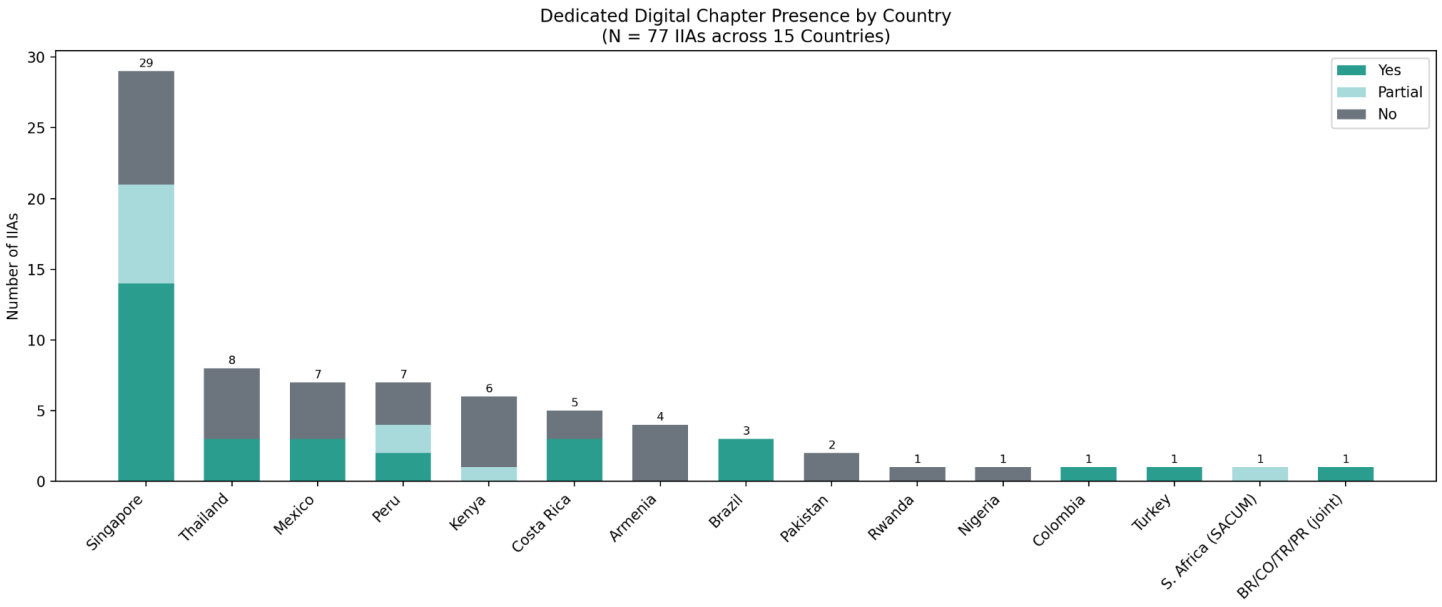


Figure 3.3: Dedicated Digital Chapter Presence by Country

3.2.2 Digital Provisions Embedded in Investment Chapters

Apart from the digital chapters, which stand alone, there is also an important segment of the database in which the digital provisions are contained in the investment chapters and not in a separate digital chapter. Out of the total of 77 FTAs/BITs, 30 FTAs/BITs (38.9%) have partial digital provisions contained in the investment chapter, and only 2 FTAs/BITs (2.6%) have

comprehensive digital provisions wholly contained in the investment chapter without having a separate digital chapter. The remaining 42 FTAs/BITs (54.5%) have no digital provisions in their investment chapters.

Modality of Digital Engagement	Number of IIAs	Percentage
Dedicated Digital Chapter (Yes)	31	40.3%
Dedicated Digital Chapter (Partial)	11	14.3%
No Dedicated Digital Chapter	35	45.5%
Digital Provisions in Investment Chapter (Partial)	30	38.9%
Digital Provisions in Investment Chapter (Yes)	2	2.6%
No Digital Provisions in Investment Chapter	42	54.5%

Table 3.2 - Modalities of Digital Provision Inclusion Across 77 IIAs

3.2.3 Country-Level Patterns and Regional Observations

Several trends arise from the dataset related to the inclusion of digital chapters, inclusion based on nations and regions. The digital chapter inclusion practice in the treaties of Singapore represents the most elaborate and comprehensive form since the said chapters are contained in their DEA, TIP-FTA, and CEPA type agreements. This indicates a deliberate negotiation strategy to include the digital disciplines in its trade and investment agreements, which is consistent with its domestic Digital Economy for Action ('DEFA') and Smart Nation Initiative, both of which form the foundation of its broader objective to establish itself as a digital economy hub, as will be analyzed further in Section 4.12.[16] Meanwhile, the trend represented by the CPTPP Chapter 14 inclusion and USMCA/CUSMA impact on the digital trade standard within the region is seen through the inclusion of the digital chapter within the free trade agreement of Latin American states,

16 See Section 4.12 (Singapore: Domestic Digital Policy Framework and Treaty Practice).

particularly Peru, Mexico, and Costa Rica. In the case of Brazil, which has consistently avoided ISDS-based BITs, it involves an innovative approach in incorporating the digital economy chapter in the agreements on cooperation and facilitation of investment. Kenya, Rwanda, Nigeria, and South Africa represent some of the African states in the sample with low digital chapter inclusion. In the case of Kenya, only one out of its six treaties contains a partial digital chapter, which clearly shows that the treaty practice of these countries is trying to balance a relatively new approach to AfCFTA and old-style BITs. The EU-Armenia CEPA agreement and the EAEU Treaty are the two most important out of the four treaties signed by Armenia, and they do not contain any special digital clauses either.

3.3. Data Governance and Performance Requirements

The following section explores the prevalence of certain data governance provisions within each of the 77 selected IIAs. Three types of provision have been selected for analysis: cross-border data flow provisions, data localization clauses, and right-to-regulate provisions for digital policy. These three clauses typically aid in structuring data governance regulations within IIAs and highlight the conflict between the state's desire for control and its inclusion of protectionist measures, and the liberalization levels of investment.

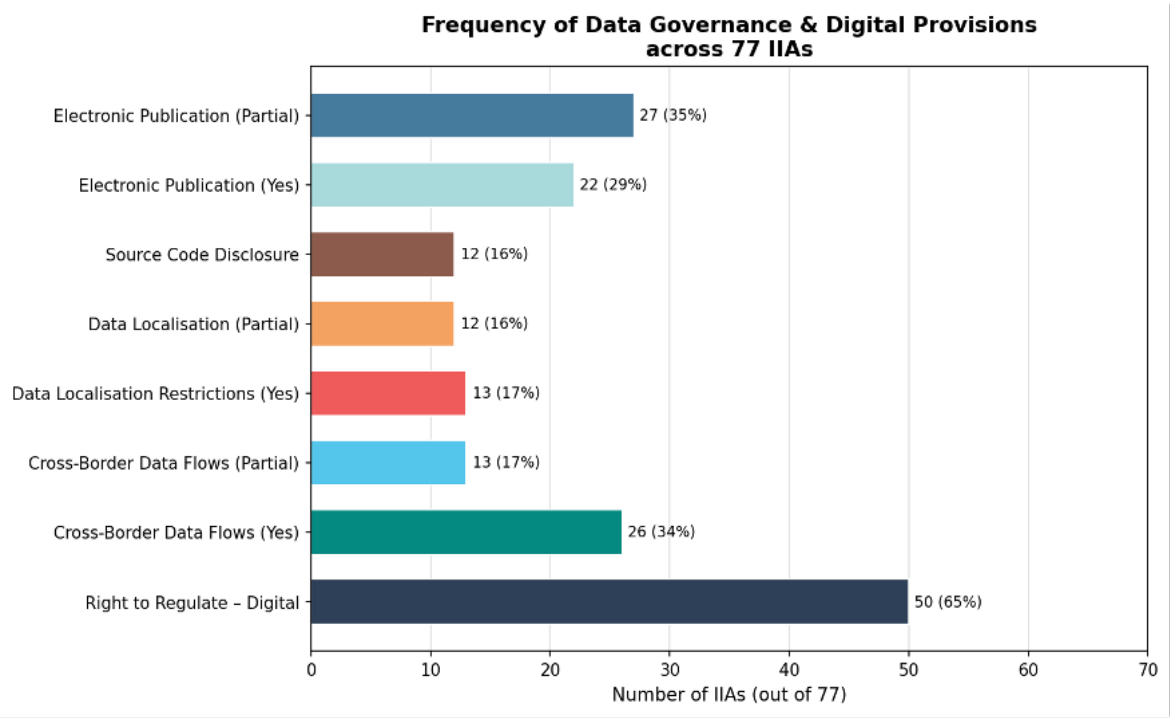


Figure 3.4 - Frequency of Data Governance and Digital Provisions across 77 IIAs

3.3.1 Cross-Border Data Flow Commitments

Of the 77 agreements examined, 26 (33.8%) contains binding cross-border data flow commitments, while another 13 (16.9%) feature partial data flow provisions, such as cooperation and market access enablement provisions. Altogether, of the selected IIAs, 39 agreements (50.6%) include some form of data flow provision. On the other hand, 38 agreements (49.4%) contain no data flow provisions.

Binding data flow commitments are also highly concentrated in agreements with Singapore, accounting for 16 of the 26 containing such provisions(61.5%). Costa Rica (3), Brazil (2), Mexico (2), Peru (2), and Thailand (2) all provide more examples of significant data flow promises. This division shows that free flow of data provision is found in the Asia-Pacific and in several Latin American Treaty practice, but is absent from the IIAs of African and Central Asian parties included in the database.

Where there is a partial commitment in the data set (13 agreements), it ends up taking either of the following forms: (i) “chapters on electronic communications” that enables data transfers through market access and interconnection rules, without explicitly referring to data flows[17]; or (ii) “cooperation provisions” that obligate the parties to facilitate data flows without creating legally binding obligations to remove such restrictions[18].

---

[17] Comprehensive and Enhanced Partnership Agreement between the European Union and the European Atomic Energy Community and their Member States, of the one part, and the Republic of Armenia, of the other part (signed 24 November 2017, entered into force 1 March 2021) [2018] OJ L23/4, Chapter 8 (Information Society and Electronic Communications): 'The Parties shall promote cooperation with regard to the development of the information society to benefit citizens and businesses through the widespread availability of information and communication technology (ICT) and through better quality of services at affordable prices' and 'The Parties shall promote cooperation between the regulators from the European Union and national regulator of the Republic of Armenia in the field of electronic communications.' <https://www.europarl.europa.eu/delegations/lv/eu-armenia-comprehensive-and-enhanced-pa/product-details/20170703DPU09427>accessed 20 April 2026. See also Section 3.4 - Armenia Country Analysis

[18] Digital Economy Partnership Agreement between the Government of Singapore, the Government of Chile and the Government of New Zealand (signed 12 June 2020, entered into force 7 January 2021) Module 4 (Data Flows and Personal Information Protection), art 4.2: 'Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person', subject to the legitimate public policy exception in art 4.2(2). This provision frames data flow facilitation as a conditional liberalisation obligation rather than a hard prohibition on restriction, distinguishing it from the cooperation-only approach of EU-style agreements. <https://www.mfat.govt.nz/assets/Trade-

3.3.2 Data Localization Restrictions

Thirteen agreements (16.9%) contain explicit restrictions on data localization requirements - defined as an obligation to store or process data domestically as a condition of market access. A further Twelve (12) agreements (15.6%) feature some form of partial coverage typically through aspirational language rather than hard prohibitions. On the other hand, the discipline is entirely absent from 52 agreements (67.5%).

The greatest proportion of data localization provisions is found in Singapore, with seven (7) agreements that contains explicit anti-localization prohibitions, and seven (7) agreements that provides partial discipline, accounting for around 54% of all such provisions recorded across seventy-seven (77) IIA in the dataset. Mexico follows with 2 full entries, and Brazil, Colombia, Costa Rica, and Peru each contribute 1 full entry in the data set. Thailand shows 3 partial localization provisions, reflecting an intermediate approach that acknowledges localization concerns without adopting hard prohibitions. Anti-localizations have been opposed by countries possessing large-scale industry in data-intensive sectors or facing internal pressures to protect their data sovereignty. For that reason, the lack of any data localization limits in the dataset's African and Central Asian agreements is unsurprising.

3.3.3 Right to Regulate Clauses Relating to Digital Policy

A significant number of data governance provisions are represented by ‘right-to-regulate’ clauses, which are part of the treaty system, allowing states to legislate and implement measures to achieve legitimate public policy objectives. Of the 77 agreements analyzed, right-to-regulate provisions were found in 50 (64.9%). Two other agreements offer some right-to-regulate provisions, and 21 agreements (27.3%) lack any such provisions.

Country-by-country analysis indicates that right-to-regulate provisions are widely in place even when the country in question does not actively engage in digital chapters in international trade. This is evidenced by Peru's inclusion of such provisions in all 7 of its agreements, Armenia's in all 4, and Brazil's in all 3. This shows that protecting one’s capacity to regulate more generally or in

agreements/DEPA/DEPA-Chile-New-Zealand-Singapore-21-Jan-2020-for-release.pdf>accessed 20 April 2026. See also Section 3.15 - Singapore Country Analysis

relation to digital policy remains an almost universal practice when drafting treaties.. Singapore includes right-to-regulate provisions in 21 of its 29 agreements.

Provision Type	Yes	%	Partial	%	No	%
Cross-Border Data Flows	26	33.8%	13	16.9%	38	49.4%
Data Localization Restrictions	13	16.9%	12	15.6%	52	67.5%
Source Code Disclosure	12	15.6%	N/A	-	65	84.4%
Right to Regulate – Digital	50	64.9%	2	2.6%	21	27.3%
Electronic Publication	22	28.6%	27	35.1%	20	26.0%
Technology Transfer	10	13.0%	1	1.3%	62	80.5%

Table 3.3 - Data Governance Provisions Across 77 IIAs

4. Domestic Digital Policy and Treaty Interaction

This section offers country-level analysis to examine how domestic digital policies and IIAs interact and influence one another. Each country's case study follows a set structure: first, it outlines the domestic digital policy framework, including strategies, policies, laws, and institutions. Second, it will review the country's treaty practice, focusing on the presence of digital provisions in IIAs. Lastly, it will examine the interaction between the domestic policies and IIA practice by assessing whether the treaty commitments reflect domestic priorities.

The sample includes the following countries: Armenia, Brazil, Colombia, Costa Rica, Kenya, Mexico, Nigeria, Pakistan, Peru, Rwanda, Saudi Arabia, Singapore, South Africa, Thailand, and Türkiye. They were selected based on the criteria identified by UN Trade and Development (2025). The UN Trade and Development (2025) report describes the listed countries as having relatively

mature or evolving digital regulatory frameworks and increasingly participating in agreements addressing digital issues. The selected countries also have diverse geographies and systems, allowing us to gain a broader understanding of how certain areas and systems interact with digital policies and trade.

This section will not contain exhaustive country profiles, as it will focus on identifying comparative patterns in how domestic policies and treaty practices interact.

4.1. Armenia

Armenia presents a case of internationally influenced digital governance where treaty frameworks shape domestic policy rather than the reverse. The country has positioned its ICT sector as a driver of economic modernization, with the sector accounting for 20 percent of commercial services exports and attracting global firms such as Adobe, Cisco, and NVIDIA. Notably, Armenia does not impose blanket data localization requirements, permitting cross-border transfers subject to adequate safeguards. At the treaty level, Armenia's BIT network remains traditional in structure with no explicit digital provisions. A notable gap persists between the country's advancing domestic framework and the limited digital content of its BITs, which all predate its digital strategy instruments.

A. Domestic Digital Policies

Armenia has positioned digital transformation as a central component of its national development strategy, reflecting the country's ambition to leverage its ICT sector as a driver of economic modernization. The sector already accounts for 20 percent of commercial services exports, and the trade presence of global firms such as Adobe, Cisco, and NVIDIA signals growing credibility as a regional digital hub.[19]

To manage this growth, the government has established an institutional architecture to support the digital economy. Responsibilities are divided between the Ministry of High-Tech Industry, which sets policy and strategy, and the Information Systems Agency of Armenia ('ISAA'), which

[19] 'Armenia–Digital Economy' (International Trade Administration, 16 December 2025) <https://www.trade.gov/country-commercial-guides/armenia-digital-economy\>.

implements digital government initiatives.[20] The principal strategic instrument at the national level is the Digitalization Strategy of Armenia for the period 2021-2025 ('DSA'), adopted in February 2021.[21] Its key objectives include the digital transformation of public administration, the implementation of a digital governance framework overseeing the development and usage of digital services, and the digitalization of public services to improve citizen engagement and accessibility of essential services. However, the OECD notes that coordination challenges remain, particularly following institutional restructuring that has affected SME support services.[22] This gap between strategy and implementation highlights a broader challenge, as digital strategies signal commitment to investors but their impact ultimately depends on effective institutional capacity.

In the area of data protection, Armenia's primary legislative instrument is the Law on Protection of Personal Data, which entered into force on 1 July 2015.[23] The law regulates the collection, processing, storage, transfer, and protection of personal data, establishing fundamental rights for data subjects and obligations for data processors. Importantly, the law does not impose blanket data localization requirements, although cross-border transfers are subject to conditions administered by the Personal Data Protection Agency.

Another development occurred through the introduction of comprehensive cybersecurity legislation. On 14 August 2024, the Government approved a package of draft laws comprising the Law on Cybersecurity, the Law on Public Information, and the Law on the Information Systems Regulatory Body.[24] The cybersecurity law defines vital sectors and critical information infrastructure in both the public and private sectors, establishes criteria based on risk and impact assessment, and mandates compliance with specific standards, including ISO 27001. It also

[20] SIGMA, 'Service Delivery and Digitalisation: Public Administration in Armenia 2025' (OECD Publishing 2025).

[21] Digitalisation Strategy of Armenia 2021–2025 (Appendix 1 of Armenian Government Decision N183-L, 11 February 2021).

[22] OECD, Advancing the Digital Transformation of Armenian Businesses (OECD Publishing 2024) 3–4.

[23] Law of the Republic of Armenia on Protection of Personal Data (Law No HO-49-N, adopted 18 May 2015, entered into force 1 July 2015). The law implements the constitutional guarantee of personal data protection under art 34 of the Constitution of the Republic of Armenia 2015.

[24] Information Systems Agency of Armenia, 'The Government has approved the package of draft laws presented by the Ministry of High-Tech Industry, including the draft law "On Cybersecurity"' (14 August 2025) <https://isaa.am/en/articles/%D5%B6%D5%B8%D6%80%D5%B8%D6%82%D5%A9%D5%B5%D5%B8%D6%82%D5%B6%D5%B6%D5%A5%D6%80/the-government-has-approved-the-package-of-draft-laws-presented-by-the-ministry-of-high-tech-industry-including-the-draft-law-on-cybersecurity\> accessed 19 March 2026.

provides for the establishment of a National Cybersecurity Agency, which will serve as the central point of contact for incident response, awareness-raising, and information-sharing.[25] The cybersecurity legislative package represents a significant maturation of the country's digital governance framework.

Overall, Armenia's domestic digital policy framework is characterised by a trajectory of progressive institutionalization and regulatory development. While the country has made considerable strides in establishing the strategic and legal foundations for digital transformation, challenges persist in areas such as SME digitalization, uneven adoption of digital public services, and the need for further alignment of cybersecurity and e-signature standards with EU and international norms.

Year	Instrument	Type
1995-2019	Network of bilateral investment treaties (BITs)	Treaty (bilateral)
2015	Law on Protection of Personal Data	Domestic legislation
2017	EAEU Digital Agenda until 2025	Treaty (regional)
2021 (Feb)	Digitalization Strategy of Armenia 2021-2025	Domestic strategy
2021 (Mar)	EU-Armenia CEPA (entry into force)	Treaty (partnership)
2024 (Sept)	Cybersecurity legislative package	Domestic legislation

Table 4.1.1 - Timeline of Key Domestic and Treaty Instruments

B. Treaty Practice in the Digital Sphere

Armenia's treaty practice in the digital sphere is shaped by two principal vectors of international economic engagement: its membership in the Treaty on Eurasian Economic Union ('EAEU'), and its Comprehensive and Enhanced Partnership Agreement ('CEPA') with the European Union, signed on 24 November 2017 and entering into force on 1 March 2021.[26] The treaties in discussion for this section are the following:

(1) CEPA;

[25] Albert Nerzetyan, 'Building the Architecture of Cybersecurity: Armenia's Institutional Turn' (EVN Report, 19 November 2025). The law was passed in first hearing by the National Assembly in September 2024.

[26] European Parliament, *EU–Armenia Comprehensive and Enhanced Partnership Agreement (CEPA)* <https://www.europarl.europa.eu/delegations/lv/eu-armenia-comprehensive-and-enhanced-pa/product-details/20170703DPU09427> accessed 19 March 2026.

(2) the EAEU;

(3) the Armenia - Singapore Agreement on Trade in Services and Investment ('ASA');

(4) the CIS Agreement on Services and Investment ('CISA'); and

(5) the EU-Armenia Comprehensive and Enhanced Partnership Agreement ('EUACEPA').

In addition, Armenia maintains a significant network of BITs, although these remain largely traditional in their orientation and do not typically contain explicit digital economy provisions.

The CEPA does not contain a dedicated digital trade chapter, but, instead, digital and electronic matters are integrated into the services chapters. The agreement addresses it within the E-commerce section of the Services Chapter (Chapter 5) and the Information Society Chapter (Chapter 8).[27] Importantly, CEPA contains regulatory approximation provisions that create a pathway for the EU's digital governance model to shape Armenian domestic law.

In parallel, Armenia's regulatory landscape is also shaped by its membership in the EAEU, which began in January 2015. The 2017 EAEU Digital Agenda serves as the primary driver of digital development in this sphere, emphasizing interoperability, electronic signature recognition, and shared digital platforms to facilitate regional trade.[28] Though these goals overlap with EU interests, the underlying strategy prioritizes Eurasian integration over European convergence. Consequently, Armenia must navigate two different institutional logics: one driving toward European standards and the other toward Eurasian harmonization.

Armenia's BITs do not typically include explicit references to the digital economy, digital trade, data governance, or data localization requirements. The absence of digital-specific provisions is consistent with the broader observation that the vast majority of existing IIAs were negotiated for an analogue economic environment and include little normative guidance on the treatment of digital forms of investment. Foreign investors in Armenia's growing digital economy must therefore rely on the general provisions of existing BITs - such as fair and equitable treatment ('FET') and full protection and security ('FPS') - supplemented by the more specific digital

[27] EU–Armenia CEPA (2017) ch 5 and 8.

[28] Decision of the Supreme Eurasian Economic Council No 12, 'Main Directions for Implementing the Digital Agenda of the Eurasian Economic Union Until 2025' (11 October 2017).

economy provisions of the CEPA and the EAEU framework, to structure and protect their investments. FEP, for example, can discipline the conduct of States that affect digital investment, in particular where regulatory mechanisms may undermine investors' legitimate expectations of having a predictable legal landscape.[29]

Policy Domain	Domestic Framework	Treaty Provisions (CEPA / EAEU / BITs)	Alignment
Data protection	Law on Protection of Personal Data (2015): rights-based framework regulating collection, processing, storage and transfer.	CEPA: dialogue on consumer protection in e-commerce (non-binding). EAEU: emerging data governance coordination. BITs: silent.	Partial
Data localization	No blanket data localization requirement imposed under domestic law.	CEPA: implicitly favours open data flows. EAEU: no localization mandate. BITs: no provisions.	Aligned
Cybersecurity	Cybersecurity law package (2024): defines critical infrastructure, mandates ISO 27001, establishes independent National Cybersecurity Agency.	CEPA: no binding cybersecurity disciplines. EAEU: interoperability and incident-response coordination. BITs: silent.	Gap
E-signatures	Domestic e-signature framework in place; alignment with EU eIDAS ongoing.	EAEU: mutual recognition as priority under Digital Agenda. CEPA: regulatory approximation pathway. BITs: silent.	Partial
Source code	No domestic legislation on source code disclosure.	CEPA: not addressed. EAEU: not addressed. BITs: not addressed.	Absent
Cross-border data flows	Permitted under the Data Protection Law subject to adequate safeguards.	CEPA: regulatory dialogue on cross-border certification. EAEU: common digital platforms. BITs: not addressed.	Partial
Digital infrastructure	DSA 2021–2025: unified platform integration, digital public services, cross-government standards.	CEPA: development cooperation provisions. EAEU: common digital platforms. BITs: broad asset definitions may cover digital assets but no specific provisions.	Gap
SME digitalization	DSA identifies SME digitalization as a priority; OECD notes persistent implementation challenges.	CEPA: development cooperation channel. EAEU: no specific SME digital provisions. BITs: silent.	Gap

Table 4.1.2 - Domestic Digital Policy vs Treaty Provisions: Comparative Overview

[29] *Tecnicas Medioambientales Tecmed SA v United Mexican States* (Award) ICSID Case No ARB(AF)/00/2 (29 May 2003) paragraph 154.

C. Domestic law-IIA Interaction

As is displayed by the table above, the relationship between Armenia's domestic digital policies and its treaty commitments is broadly complementary, though the degree of alignment varies across policy domains. Three patterns stand out.

First, where domestic frameworks are already aligned with treaty disciplines, Armenia has accepted those disciplines without conflict. The clearest example is data governance. Armenia's Data Protection Law of 2015 and its adherence to Council of Europe Convention 108 and Convention 108+[30] create a regulatory environment that is broadly compatible with both the CEPA's provisions on electronic commerce and the EAEU's emerging digital trade framework. Similarly, Armenia's decision not to impose strict data localization requirements is consistent with the open data flow principles implicit in both the CEPA and the EAEU's digital agenda. Because Armenia does not apply a blanket localization mandate domestically, it has been able to engage with both treaty frameworks without requiring domestic legislative reform - a structural advantage that countries with strict localization regimes do not share.

Second, the direction of influence between domestic policy and treaty obligations is predominantly international-to-domestic. The CEPA's regulatory approximation provisions create an explicit mechanism for the EU's digital governance standards to shape Armenian law. The EAEU Digital Agenda exerts a parallel pull. Armenia thus finds itself navigating between two competing standards of digital integration, and commentators have observed that its EAEU membership obligations may at times create tensions with its digital partnership commitments to the EU.[31] For example, where EAEU interoperability requirements on electronic signatures diverge from EU eIDAS standards, Armenia faces the practical challenge of maintaining compatibility with both frameworks. To date, however, these tensions have remained latent rather than resulting in any direct legal conflict.

---

[30] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108, opened for signature 28 January 1981, ETS No 108); Protocol amending the Convention (Convention 108+, opened for signature 10 October 2018, CETS No 223).

[31] Hrant Kostanyan and Richard Giragosian, *EU-Armenian Relations: Charting a Fresh Course* (CEPS Research Report No 2017/14, 2017) <https://ssrn.com/abstract=3075166> accessed 19 March 2026.

Third, a notable gap exists between Armenia's advancing domestic digital governance framework and the limited digital content of its BITs. As the timeline in Table 1 shows, all of Armenia's BITs predate its digital strategy instruments. As Armenia's digital economy continues to grow, the absence of digital-specific investment protections in its BIT network represents a significant gap. The CEPA and EAEU frameworks partially fill this gap through their digital governance provisions, but they do not substitute for the kind of investor protections that modernised BITs could provide.

In summary, Armenia's domestic-treaty interaction in the digital sphere is characterised by a progressive, if uneven, alignment between its developing domestic digital governance framework and its international obligations. The primary direction of influence appears to operate from the international level to the domestic level, rather than Armenia exporting a distinct national digital governance model through its treaties.

4.2. Brazil

Brazil's digital policy and treaty practice are mainly development-oriented. They are selectively liberalized, with certain policies focused more on nationalistic endeavors, and domestically use digitalization as a means to broaden their industrial and economic strategy. Brazil avoids data localization, but has public oversight and its treaty practice is progressively liberal. The treaties also have provisions on cross-border data flow and data localization restrictions. However, not all treaties are uniform, as MERCOSUR Agreements rely more on cooperation and capacity-building. The interaction between its domestic policy and treaty practice, therefore, seems to be a flexible one, with its domestic practice supporting industrial development and technological sovereignty, and its treaties supporting digital trade, integration, and cooperation.

A. Domestic Digital Policy Framework

The Laws and policies in Brazil show that the country is increasingly integrating digital provisions into sectors such as industrial policy, data governance, AI strategy, cybersecurity, and platform regulation. These policies and laws demonstrate that Brazil has a comprehensive approach to digital reform, making digital policy central to national and industrial development.

At the national level of development planning, Brazil's recent policy architecture is clearly tied to industrial transformation and development. The Nova Indústria Brasil (New Industry Brazil) (2024) treats digitalization as part of the national industrialization strategy with polices such as the industrial program that is running to 2033, built around innovation and sustainability, with six missions, priority investment areas, and R$300 billion in financing available through 2026. The policy seems to be stimulating technological development by increasing industrial competitiveness and strengthening Brazil's qualified participation in international markets. Within the policy's umbrella, Brasil Mais Produtivo allocates R$2 billion to the digital transformation of micro, small, and medium industries, suggesting that Brazil aims to transform its industries through greater digitization.

There is also the Brazilian National AI Plan (2024), a policy that aims to approach AI strategy with an investment framework. The 2024 plan is organized around five axes: (1) infrastructure and AI development; (2) diffusion, training, and capacity-building in AI; (3) AI for improving public services; (4) AI for business innovation; and (5) support for AI regulation and governance. Overall, the plan projects R$23.03 billion in investment for 2024-2028, of which R$5.79 billion is allocated to the first axis, which includes a national AI infrastructure program, a sustainability and renewable-energy program for AI, a data and software ecosystem program, and AI research and development funding.

The Brazilian Digital Transformation Strategy (2022-2026) (E-Digital) frames digitization as national transformation, linking digitization to multiple sectors, including commerce, research, health, industry, the public sector, finance, security, energy, transport, and media. This results in data becoming a core input for both public governance and private production.

The National Internet of Things Plan, instituted by Decree No. 9,854 of 2019, makes even clearer how Brazil combines openness and liberalization with its governance safeguards (allowing space for the government to make its exceptions). According to the Ministry of Science, Technology, and Innovation, the plan was created to implement and develop the Internet of Things in Brazil "*based on free competition and the free flow of data*," while also observing information security and personal data protection guidelines.

The Industrial Policy for the ICT Sector (Decree No. 10,602 of 2021) targets domestic value added, R&D investment, national technology, productivity, employment, public procurement of ICT and semiconductors, integration into manufacturing, reducing inequalities, and pursuing technological sovereignty. ICT policy is treated as industrial policy to strengthen domestic technology production. The 2024 ICT and semiconductor policy, however, links semiconductors to technological sovereignty, supports research, development, innovation, production, and encourages public procurement of nationally produced ICT goods. This shows Brazil's desire to shift its digital policy toward prioritizing domestic capability and autonomy.

Law No. 13.709 of 2018 on the General Data Protection Law, which entered into force in 2022, is the core of Brazil's data governance model. The law regulates data protection without imposing a blanket data localization ban. Additionally, Law 12.965, the Civil Rights Framework for the Internet, establishes the principles and rights that govern internet use in Brazil, positioning Brazil's digital framework as rights-based.

Federal Decree Number 7.962/13 on E-Commerce Contracting applies the Consumer Defense Code to electronic commerce contracting. Its main role is to strengthen trust in online markets by regulating disclosure, consumer information, and transactional standards.

Finally, Law 14.478 on the Provision of Virtual Asset Services mentions crypto-assets and digital finance. The Law contains principles regarding information security, personal data protection, consumer protection, financial integrity, and anti-money laundering. Altogether, these policies and laws show how well developed Brazil's domestic digital framework is and how it focuses on development and innovation.

Year	Instrument	Type
2013	Federal Decree No. 7.962 (E-Commerce Contracting)	Domestic law
2018	Brazil–Chile Free Trade Agreement	Treaty
2019	National IoT Plan (Decree No. 9.854)	Domestic policy
2021	ICT Industrial Policy (Decree No. 10.602)	Domestic policy
2021	Mercosur E-Commerce Agreement	Treaty
2022	LGPD enters into force	Domestic law
2023	MERCOSUR–Singapore FTA	Treaty
2024	Nova Indústria Brasil	Domestic policy
2024	Brazilian National AI Plan	Domestic policy
Ongoing	WTO JSI	Plurilateral

Table 4.2.1 Timeline of Key Domestic and Treaty Instruments

B. *Treaty Practice in the Digital Sphere*

Brazil, as is reflected by its usual pattern of treaty practice in international economic law, by showing its usual cautiousness on its treaty commitments in addition to its usual alignment with domestic development, only has a small cluster of trade agreements within the digital sphere.[32] These agreements are the:

(1) Free Trade Agreement between Brazil and Chile (2018);
(2) the Free Trade Agreement between MERCOSUR and Singapore (2023);
(3) the Mercosur E-Commerce Agreement (2021); and
(4) the WTO Joint Statement Initiative on Electronic Commerce (ongoing plurilateral negotiations).

The Brazil-Chile FTA, signed in 2018 and entered into force in 2022, is Brazil's most advanced digital treaty. It includes a Digital Trade Chapter that establishes foundational principles for e-commerce and digital trade. One of these key provisions concerns cross-border data flows, detailed in Article 10.12(2), stating 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."*

This clause favors cross-border data flows, which is crucial for modern digital trade agreements. However, the provision also includes regulatory safeguards that allow parties to adopt measures with legitimate public policy objectives, including privacy protection. The agreement also contains provisions addressing data localization, stating in Article 10.13(2) of the agreement that:

> *"A Party may not require a person of the other Party to use or locate computer facilities in the territory of that Party as a condition of doing business in that territory."*

This is consequential as it limits a country's ability to mandate data localization, indicating that Brazil aligns with the emerging norm favoring cross-border data flows over ultra-protectionist

[32] Sanchez Badin, Michelle Ratton, and Fabio C. Morosini. "Re-conceptualizing International Investment Law from the Global South." *Morosini, Fabio* (2017): 11-14

measures. The agreement also includes provisions that protect source codes and commitments relating to electronic authentication and electronic signatures, consumer protection in electronic commerce, online personal data protection, and paperless trading. These provisions show that the Brazil-Chile agreement is a very comprehensive digital trade instrument.

The MERCOSUR-Singapore FTA, entered into force in 2026, similarly contains a dedicated Electronic Commerce Chapter. Brazil is a member of the South American MERCOSUR trade bloc, along with Argentina, Paraguay, and Uruguay. In comparison, the MERCOSUR-Singapore FTA is less advanced than the Brazil-Chile agreement, as its provisions do not address matters in the digital economy, such as cross-border data flows, data localization restrictions, or source code disclosure protections. Instead, the chapter contains provisions such as digital trade facilitation, consumer protection, interoperability of electronic transactions, regulatory cooperation, and cybersecurity collaboration. For instance, a core rule in the chapter is recognition of electronic contracts. Article 12.3(1) of the agreement states:

> *"Each State Party shall not deny the legal validity of a transaction, including a contract, solely on the basis that the transaction is in electronic form."*

The agreement also protects the legal recognition of electronic signatures and authentication methods in Article 12.4(1), which states:

> *"A State Party shall not deny the legal validity of a signature solely on the basis that the signature is in electronic form."*

The same provision also prevents governments from restricting authentication technologies chosen by contracting parties (Article 12.4(2)(a)):

> *"A State Party shall not adopt or maintain measures for electronic authentication that would prohibit parties to an electronic transaction from mutually determining the appropriate authentication methods for that transaction."*

The chapter also has provisions on paperless trading and electronic invoicing. Lastly, the chapter has provisions on digital and cybersecurity cooperation.

The provisions in this agreement are much less legally prescriptive than the Brazil-Chile provisions on data flows and localization, as, instead of establishing strict prohibitions or obligations, the MERCOSUR–Singapore agreement often uses soft language such as "shall endeavour to cooperate" or "shall exchange information and best practices."

Nonetheless, the agreement does include provisions addressing electronic transactions. These provisions indicate that, while the MERCOSUR–Singapore agreement includes provisions on digital trade governance, it does so through a cooperation-oriented model rather than a market-liberalization model.

The Mercosur E-Commerce Agreement, entered into force in 2023, is entirely different from the previous agreements. Instead, it is a regional effort to harmonize digital trade governance within the Mercosur bloc, focusing primarily on creating a regulatory framework for digital commerce across the member states. The agreement addresses issues such as electronic contracts, consumer protection in online markets, and the recognition of electronic signatures. It also focuses on regulatory cooperation and policy coordination among member states, and promotes the development of digital trade infrastructure and the alignment of domestic regulatory frameworks. The Mercosur E-Commerce Agreement, in fact, reflects how Brazil may be focused on institutional cooperation, regulation, and capacity-building rather than liberalization.

Brazil also participates in the JSI. The JSI is currently the most important plurilateral agreement that is still being developed in digital trade. It was created to develop common rules governing digital trade, including cross-border data flows, electronic authentication, consumer protection, and cybersecurity. The negotiations are still ongoing, but Brazil's participation shows that it is willing to engage in multilateral agreements on digital trade.

Overall, Brazil's digital treaty commitments are mostly located in its dedicated digital trade chapters rather than in investment provisions. Furthermore, Brazil has not made similar levels of commitment in each agreement. While the Brazil-Chile FTA is very advanced and contains many commitments, the others do not. Lastly, the provisions throughout the agreements are development-oriented, including commitments or ambitions to build capacity and collaborate.

Policy Domain	Domestic Framework	Treaty Provisions	Alignment

Data protection	LGPD (2018) regulates data processing and rights	Brazil–Chile: personal data protection provisions	Aligned
Data localization	No blanket localization ban	Brazil–Chile: prohibits localization requirements	Aligned
Cross-border data flows	Permitted under the domestic framework	Brazil–Chile: explicit allowance	Aligned
Source code	Not strongly regulated domestically	Brazil–Chile: protection provisions	Partial
E-commerce regulation	Decree 7.962/2013 governs consumer protection	All agreements include e-commerce provisions	Aligned
Digital infrastructure	Strong ICT and industrial policies	Mercosur agreements focus on cooperation	Partial
AI governance	National AI Plan (2024)	Limited treaty references	Gap
Cybersecurity	Mentioned in domestic strategies	Treaty provisions mostly cooperative	Partial

Table 4.2.2 Domestic Digital Policy vs Treaty Provisions: Comparative Overview

C. *Domestic Law – IIA Interaction*

Comparing Brazil's domestic digital policies with its treaty practices on the same topic shows that the treaties reflect its domestic policy priorities. However, the treaties are clearly not a reproduction of domestic laws and policies; nevertheless, the interests align, as Brazil seems to internationalize its domestic strategy while still preserving its regulatory autonomy. For instance, the domestic policies, such as Nova Indústria Brasil, demonstrate Brazil's commitment to digital transformation, especially as a means of economic development. This can also be viewed in the treaties such as the Brazil-Chile FTA and the MERCOSUR-Singapore FTA.

In fact, Brazil's domestic data governance framework, centered on the General Data Protection Law and the Marco Civil da Internet, also appears compatible with Brazil's treaty commitments. Unlike some jurisdictions with strict data localization rules, Brazil's data governance model focuses on privacy protection and responsible data processing, without territorial restrictions on data flows, both domestically and under treaties. Although Brazil's domestic regulatory model does not impose strict localization rules, treaty commitments that restrict localization do not necessarily conflict with existing domestic laws and policies.

Furthermore, there are restrictions on digital liberalization, as many agreements do not include binding commitments on issues such as data localization or source code protection, relying instead on cooperation clauses. Brazil, as such, is selective on certain provisions. This selectiveness is also

evident in policies such as the ICT and semiconductor industrial policies, which emphasize technological sovereignty and domestic capability-building. However, these provisions still do not oppose the treaties Brazil has committed to.

Brazil still seems to be reserving policy space in areas related to digital infrastructure, and advanced technology is strategically important. Therefore, Brazil appears to have adopted a strategic flexibility approach in digital treaty-making by accepting digital trade rules that facilitate innovation and market participation while avoiding commitments that could constrain its ability to pursue industrial and technological policy objectives.

Lastly, on the JSI, Brazil's participation reflects the state's willingness to engage in multilateral rule-making while also maintaining some flexibility in binding commitments. Furthermore, on other matters, explicit domestic policy mention is absent on source code, which contrasts with the stronger protections found in certain treaties, resulting in only partial alignment.

In conclusion, it does not seem that Brazil's treaty practices export any specific domestic models, as it appears to have different commitments depending on the context and partner. For instance, the Brazil-Chile FTA is negotiated bilaterally with a partner that actively promotes digital trade governance[33] and contains strong digital provisions, while agreements negotiated within Mercosur frameworks tend to rely more heavily on cooperative language. This suggests that Brazil's digital treaty practice is context-sensitive.

4.3. Colombia

Domestically, Colombia uses digitalization as a tool for economic growth and governance modernization. Colombia's domestic goals include bridging the digital divide and promoting data governance that enables cross-border transfers, which is very compatible with its treaty practice, which also includes provisions on electronic signatures and consumer protection, while still preserving regulatory autonomy through public policy exceptions. Colombia has a very development-oriented approach and uses international agreements to support digital economic integrations, but also maintains flexibility in order to pursue domestic innovation goals.

[33] WTO, *Integrated Support Initiatives Propel Chile's Digitally Delivered Services Exports* (2025) 3–4 https://www.wto.org/english/tratop_e/ts4d_e/case_studies_e/chile.pdf accessed 28 March 2026.

A. Domestic Digital Policy Framework

Colombia has numerous development-oriented digital policies and laws, and digitization is a crucial topic in the National Development Plan 2022–2026, which aims to set guidelines for Colombia's growth and development, positioning technology, AI, and digital connectivity as core drivers for social equity, energy transition, and productive transformation. The National Development Plan aims to do this by integrating digital technologies across all sectors.

Colombia's other policies also work towards development-oriented digital policies. For instance, the New Science, Technology, and Innovation Policy (CONPES 4069) 2022–2031 is a long-term roadmap for technological development that seeks to increase contributions to science, technology, and innovation for Colombia's "*social, economic, environmental, and sustainable development*". Therefore, Colombia seeks to strengthen its research capacity and expand the role of digital technologies in its economy, thereby promoting its markets as knowledge-based.

Colombia also has a National Digital Strategy 2023–2026, which focuses on expanding connectivity, accelerating digital transformation, and enhancing economic growth through technology. One of the goals of this strategy is to close the digital divide in Colombia.

The National AI Strategy establishes the policy direction for the development, adoption, and regulation of AI, seeking to promote AI research and development. Importantly, the strategy also includes governance mechanisms to mitigate AI-related risks, such as harms to privacy or public trust. Another AI-related strategy is the Ethical Framework for AI, which has guiding principles for the ethical development and deployment of AI. The Data Sandbox Platform is the GovTech ecosystem for AI implementation, and regulatory sandboxes for AI governance promote the use of innovative digital technologies in public administration to improve public services.

Colombia also developed a Big Data Policy Framework that promotes data-driven innovation and encourages the use of data analytics in public administration. The policy also identifies structural barriers to effective data governance, including limited interoperability across government institutions and insufficient digital skills.

Colombia's laws also pursue the same aim of utilizing digitization as a method of development. Colombia's data governance model, Law 1581 of 2012, establishes the general legal framework

for the protection of personal data by regulating the collection, storage, and processing of personal data and recognizing individuals' rights over their personal information. Importantly, the law does not impose comprehensive data localization requirements.

Decree 620 of 2020 is a digital government policy that establishes guidelines for the use and operation of the digital citizen service and promotes digital transformation, enabling interoperability, digital authentication, and secure digital folders for citizens. Decree 1078 of 2015 also regulates the development of digital infrastructure and telecommunications services and Law 2069 of 2020 (Entrepreneurship Law) tries to strengthen the country's innovation ecosystem by promoting entrepreneurship and supporting the development of startups and small technology enterprises.

These laws demonstrate that Colombia's digital policies and laws are focused on innovation and development. They also promote digital transformation while still maintaining governance mechanisms that ensure data protection and ethical use of AI.

Year	Instrument	Type
2012	Law 1581 (Data Protection Law)	Domestic law
2015	Decree 1078 (ICT Sector Regulation)	Domestic law
2020	Decree 620 (Digital Government)	Domestic policy
2020	Law 2069 (Entrepreneurship Law)	Domestic law
2022	National Development Plan (2022–2026)	Domestic policy
2022	CONPES 4069 (Innovation Policy)	Domestic policy
2023	National Digital Strategy	Domestic policy
2023	Pacific Alliance–Singapore FTA	Treaty
Ongoing	WTO JSI on Electronic Commerce	Plurilateral

Table 4.3.1 Timeline of Key Domestic and Treaty Instruments

B. Treaty Practice in the Digital Sphere

Colombia has few digital treaties, even fewer than Brazil's. From the existing treaties, Colombia's commitments seem to balance the promotion of the digital market with the need to preserve

regulatory flexibility, similar to many developing economies.[34] The agreements that will be examined involving Colombia are the following:

(1) the Pacific Alliance-Singapore Free Trade Agreement; and
(2) the WTO Joint Statement Initiative on Electronic Commerce (JSI).

As with the agreements Brazil has committed to, digital provisions appear in their own dedicated electronic commerce or digital trade chapters.

The Pacific Alliance-Singapore FTA is the most comprehensive digital trade agreement involving Colombia. The agreement includes an Electronic Commerce Chapter that sets out legal rules governing digital trade and electronic transactions between the parties. An important provision is the provision on cross-border data flows. The agreement, in Article 13.14(1) on Cross-Border Transfer of Information, provides 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."*

This provision is a reflection of many modern digital agreements that aim to facilitate the free flow of data across borders.[35] However, predictably, the agreement also preserves regulatory autonomy by allowing necessary measures to be adopted for legitimate public policy objectives, such as privacy protection and cybersecurity. This is a space that must be left in any agreement to allow governments space to implement their own policy agendas that support their economy.

The agreement also includes a provision on the legal validity of electronic signatures. For example, Article 13.13(1) on Electronic Authentication provides that, if not provided by law:

> *"..., no Party shall deny the legal validity of a signature solely on the basis that the signature is in electronic form."*

This provision is crucial for facilitating cross-border digital trade (as such agreements make digital trade more accessible). The chapter also includes provisions on consumer protection in electronic

[34] Mira Burri, Kholofelo Kugler, Regulatory autonomy in digital trade agreements, *Journal of International Economic Law*, Volume 27, Issue 3, September 2024, Pages 397–423, https://doi.org/10.1093/jiel/jgae025
[35] Chin, Yik-Chan, and Jingwu Zhao. 2022. "Governing Cross-Border Data Flows: International Trade Agreements and Their Limits" Laws 11, no. 4: 63. https://doi.org/10.339,0/laws11040063

commerce, which encourage parties to adopt measures to protect consumers engaged in digital transactions (as stated in Article 13.8) and to cooperate with one another to address unsafe commercial practices (as stated in Article 15.7).

Colombia also participated in the JSI which addresses cross-border data flows, electronic authentication, consumer protection, and cybersecurity cooperation. Colombia's participation in the negotiations shows that it seeks to engage in multilateral digital trade governance.

Overall, Colombia's treaty practice in agreements regulating digital trade shows its progression on the issue. Even if the number of agreements is limited, the existing agreements show the principles of digital governance that Colombia aims to achieve, namely, recognition of electronic transactions, facilitation of cross-border data flows, and cooperation on cybersecurity and consumer protection.

Policy Domain	Domestic Framework	Treaty Provisions	Alignment
Data protection	Law 1581 regulates personal data	PA–Singapore: data protection + safeguards	Aligned
Data localization	No strict localization requirement	PA–Singapore: allows cross-border flows	Aligned
Cross-border data flows	Permitted under safeguards	Article 13.14 allows flows	Aligned
E-signatures	Recognized under the domestic framework	Article 13.13 ensures legal validity	Aligned
Consumer protection	Present in domestic law	Articles 13.8 & 15.7 cooperation	Aligned
Digital infrastructure	Strong policy focus	Limited treaty provisions	Gap
AI governance	Extensive domestic policies	No strong treaty provisions	Gap
Digital innovation	Sandbox + GovTech systems	Limited treaty reflection	Partial

Table 4.3.2 Domestic Digital Policy vs Treaty Provisions: Comparative Overview

C. Domestic Law - IIA Interaction

In comparing Colombia's domestic digital policies and its treaty practices, it can be concluded that there is an alignment between the two in terms of its policies and aims. However, even if the treaties complement the country's domestic strategy, they are not a replication of its domestic laws and policies.

For instance, the National Digital Strategy and the Science, Technology, and Innovation Policy prioritize developing digital infrastructure and the domestic digital economy. These objectives are

consistent with Colombia's participation in international digital trade agreements, as these agreements facilitate cross-border data flows.

Additionally, Colombia's domestic data governance policies are also compatible with its treaty commitments, as the country's personal data protection policies, established under Law 1581 of 2012, regulate the processing of personal data but do not impose a strict data localization requirement. Therefore, in this case, there is also no conflict with Colombia's domestic legal framework. On another note, Colombia's domestic legal framework does not impose strict data localization requirements, which enables compatibility with treaty provisions that do promote cross-border data flows. Furthermore, the state's participation in the JSI also demonstrates its interest in shaping emerging digital trade norms

Additionally, Colombia's treaty practice does not seem to push a specific domestic regulatory model. What can be viewed, however, is that the country adapts its commitments depending on the negotiating context, as is seen with Brazil. For instance, agreements that are negotiated within the Pacific Alliance framework focus on regional economic integration and digital trade facilitation, and include more comprehensive digital provisions than earlier trade agreements.[36]

Overall, Colombia's approach to digital treaty-making is development-oriented and compatible with its domestic strategy. Colombia participates in international digital trade in order to support digital economic integration while preserving the regulatory autonomy necessary to pursue domestic growth and technological development strategies.

4.4. Costa Rica

Costa Rica uses digital policy as a tool for higher investment attraction and export led growth. Most of the domestic policies, such as digital policy, are aligned with their international digital framework covering multiple aspects such as data protection, cyber security and AI governance which is consistently drawn from OECD principles and UNCITRAL model law. It does not impose data localization requirements and is deliberately open minded in terms of regulatory measures.

[36] Canovas Roque, Antonella Alexandra, Juan Carlos Daniel De Vinatea Murguía, Alexander David Perez Chamochumbi, Ricardo Alonso Quimper Roncagliolo, Ángela Isamar Tapia Ostos, Jeremy Yermain Torres Jauregui, and Julio Ricardo Moscoso Cuaresma. 2025. "The Pacific Alliance Integration Process: A Systematic Literature Review" Economies 13, no. 9: 255. https://doi.orincludeg/10.3390/economies13090255

Its domestic orientation is evident in its treaty making practice, with more recently concluded treaties, notably the Israel FTA(2025), containing binding nature commitments regarding cross-boarder data flow, data localization prohibition and digital trade governance. The alignment of domestic policy objectives with treaty provisions is thus evident in its IIAs with regard to trade and services. However, a gap persists in the investment dimension. Costa Rica can be described as a prudent rule taker that is consistently adapting internationally recognized trends to its context, whose treaty practice is catching up with its domestic digital aspirations.

A. Domestic Digital Policies

The domestic digital legal and policy infrastructure in Costa Rica embodies the country's larger economic infrastructure as a small, open economy that emphasises high-technology industries and FDIs. Through Executive Decree 41248, the Ministry of Science, Innovation, Technology, and Telecommunications ('MICITT') issued the Estrategia de Transformación Digital hacia Costa Rica del Bicentenario 4.0 2018-2022. This decree represents the first systemised effort to embed digitalization into the national development planning.[37] Some key pillars are to emphasise digital government and infrastructure, and have a larger enabling regulatory environment. To coordinate implementation across public institutions, it also established the High Level Commission of the Digital Government of the Bicentennial ('CANGD'). Costa Rica has also recently adopted its Estrategia Nacional de Inteligencia Artificial (ENIA) 2024-2027, led by MICITT. This signals the country's ambitious approach to ethical and responsible AI governance. Their main focus is on risk management, 5G infrastructure deployment, and positioning Costa Rica as a regional leader in trustworthy AI.[38] Both public and private stakeholder engagement were crucial to the creation of this policy, which reflects larger OECD AI principles, illustrating Costa Rica's support for globally recognised governance standards.

On the other hand, the primary instruments on data governance are still the Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales (Law No. 8968 of 2011). This has previously established a rights-based, consent-oriented framework that adheres to the fundamental

[37] MICITT, *Estrategia de Transformación Digital hacia la Costa Rica del Bicentenario 4.0 2018–2022* (Costa Rica, 2018) , (Original document in Spanish, English translation AI assisted.)
[38] MICITT, *Estrategia Nacional de Inteligencia Artificial (ENIA) 2024–2027* (San José, 2024), accessible via OECD.AI Policy Navigator, (Original document in Spanish, English translation AI assisted.)

constitutional rights of informational self-determination. PRODHAB acts as the regulatory authority and has not imposed data localization requirements. More broadly, this mirrors the export-oriented approach to digital strategy that is built on the open-economy data governance attitude.[39] The Digital Economy Navigator (2025) supports this institutional picture by confirming that Costa Rica has established consumer protection laws, cybercrime laws, data protection laws, a dedicated data protection authority, and a national cybersecurity strategy. It also scores higher than the DEN average on digital policy and governance overall.[40]

The COMEX's Roadmap for Strengthening the Semiconductor Ecosystem in Costa Rica (2024) from a more industrial lens shows how Costa Rica has been integrating digital policy into their investment recruitment. The roadmap shows regulatory simplification, intellectual property protection, and trade and investment facilitation as prerequisites for the consolidation of the country's status as a global semiconductor hub, which is further proven by its designation as the first country to be chosen as a strategic ally of the USA under the CHIPS and Science Act.[41]

Year	Instrument	Type
2011	Law No. 8968 (Personal Data Protection Law)	Domestic
2013	Qatar–Costa Rica BIT	Treaty
2018	Digital Transformation Strategy 2018–2022 (Executive Decree 41248)	Domestic strategy
2021	Central America–UK Association Agreement	Treaty (regional)
2024	COMEX Semiconductor Ecosystem Roadmap	Domestic policy
2024	Ecuador–Costa Rica Commercial Association Agreement	Treaty
2024–2025	UAE–Costa Rica CEPA (signed 2024, in force 2025)	Treaty
2024–2027	National AI Strategy (ENIA)	Domestic strategy
2025	Israel–Costa Rica Free Trade Agreement	Treaty

Table 4.4.1 Timeline of Key Domestic and Treaty Instruments

[39] *Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales*, Law No 8968 (Costa Rica, 7 July 2011), published in La Gaceta No 170 of 5 September 2011, (Original document in Spanish, English translation AI assisted.)

[40] Digital Commerce Organisation, *Digital Economy Navigator 2025 – Costa Rica Country Profile*

[41] Ministry of Foreign Trade (COMEX), *Roadmap for Strengthening the Semiconductor Ecosystem in Costa Rica* (San Jose, March 2024) 5–9

B. Treaty Practice in the Digital Sphere

The treaties in discussion in this section are the following:

(1) the Free Trade Agreement between Costa Rica and Israel (CRIFTA);
(2) the Agreement on Commercial Association between the Republic of Ecuador and the Republic of Costa Rica (CAECR);
(3) the UAE-Costa Rica Comprehensive Economic Partnership Agreement on Trade and Investment (CECEPA);
(4) the Central America-United Kingdom Association Agreement (CAUKAA); and
(5) the Costa Rica - Qatar BIT (CRQBIT).

Costa Rica's recent treaty practice demonstrates a deliberate and progressive incorporation of digital governance into international economic agreements. The most sophisticated example of this approach is the CRIFTA, signed in December 2025, which contains a standalone digital trade chapter. It bars customs duties on electronic transmissions, guarantees non-discriminatory treatment of digital products, and most significantly creates enforceable commitments preventing both restrictions on cross-border data flows and data localization mandates, each subject to a public policy carve-out.[42] Notably, the agreement's digital chapter specifically mentions Costa Rican domestic law, equating the treaty notion of "electronic signature" with "digital signature" as defined under Costa Rican statute, which is a rare case of domestic law being clearly integrated in treaty text.[43] A special chapter on digital commerce that addresses cross-border data flows, consumer protection, and transparency responsibilities is also included in the 2024 CAECR.[44] The CECEPA (signed 2024, in effect 2025) also includes a digital chapter, though it is notably limited in scope: it makes no mention of source code or data localization, and most of its commitments are best-efforts rather than binding obligations.[45]

---

[42] *Free Trade Agreement between Costa Rica and Israel* (signed 8 December 2025, not yet in force), ch 10 (Digital Trade), arts 10.13–10.14 (Original document in Spanish, English translation AI assisted.)
[43] Ibid, art 10.7
[44] *Agreement on Commercial Association between the Republic of Ecuador and the Republic of Costa Rica* (signed 2023, entered into force 2024), ch 13, arts 13.1–13.8 (Original document in Spanish, English translation AI assisted.)
[45] *Acuerdo de Asociación Económica Integral sobre Comercio e Inversión entre Costa Rica y los Emiratos Árabes Unidos*(signed 2024, entered into force 2025), ch 10 (Original document in Spanish, English translation AI assisted.)

By contrast, Costa Rica's participation in the CAUKAA (2021) offers far less in this area: the agreement contains no dedicated digital chapter, with digital governance appearing only incidentally within the services and investment provisions.[46] This reflects the agreement's roots in the earlier EU-Central America framework. Elsewhere in Costa Rica's treaty portfolio, the CRQBIT (2013) is a conventional first-generation instrument with no digital provisions whatsoever.[47] Taken together, Costa Rica's treaty portfolio reveals a pattern of incremental digitalization, with more recent instruments, particularly the Israel FTA and the agreement with Ecuador, embedding stronger and more binding digital disciplines than their predecessors.

Policy Domain	Domestic Framework	Treaty Provisions	Alignment
Data localization	No blanket localization requirement	Israel FTA: binding prohibition on localization mandates	Aligned
Cross-border data flows	Open flows permitted under domestic framework	Israel FTA: prohibition on restrictions	Aligned
AI governance	ENIA 2024–2027 - risk management, ethical AI, OECD-aligned	No treaty references to AI governance	Gap
E-commerce	No dedicated domestic e-commerce law	Ecuador agreement and Israel FTA include e-commerce provisions	Partial
Digital investment facilitation	Semiconductor Roadmap identifies facilitation as a priority	Investment chapters thin and non-binding across all IIAs	Gap
AI governance	No dedicated AI law or policy enacted	No treaty provisions on AI	Not engaged
Cybersecurity	National cybersecurity strategy in place	Israel FTA: cybersecurity cooperation provisions	Aligned

Table 4.4.2 Domestic Digital Policy vs Treaty Provisions: Comparative Overview

C. Domestic Law – IIA Interaction

The digital policy and treaty roadmap for Costa Rica are quite complementary as one influences the other bidirectionally. The latest FTA agreements show internationalization of legislation that was previously already domestically adopted. For example, Law No. 8968's open-flows, non-

[46] *Association Agreement between Central America and the Unitlocalizationed Kingdom of Great Britain and Northern Ireland* (signed 2019, entered into force 2021), Pt IV, Title III

[47] *Agreement between the Government of the State of Qatar and the Government of the Republic of Costa Rica for the Reciprocal Promotion and Protection of Investments* (signed 2010, entered into force 2013)

localization position is reflected in CRIFTA that bans data localization and data flow limitations.[48] This shows how Costa Rica enshrines domestic regulations in its international treaty obligations. The FTA's explicit cross-reference to Costa Rican domestic digital signature law also illustrates treaty text being used to reflect, not reshape, existing domestic frameworks.

Yet, there are still certain gaps that persist between domestic policy goals and treaty obligations. Costa Rica's Semiconductor Roadmap states that the digital investment facilitation is a key component of its investment recruitment strategy. This includes simplified regulatory clearances, intellectual property protections, and skilled worker immigration facilitation.[49]

However, the investment component of the CRIFTA only has very thin promotional cooperative wording that creates no obligatory digital facilitation responsibilities, no online authorization processes, and no ISDS mechanism.[50]

This gap shows a mismatch between domestic priorities and international policy, where one is not entirely translated to the other. Costa Rica's commercial negotiators have had success embedding digital disciplines in trade and services chapters. However, the equivalent ambition has not yet carried over into investment chapter commitments. Gap aside, Costa Rica is not exporting a distinctive regulatory model through its treaty practice. Its domestic strategy and its treaty frameworks both draw from the same internationally acclaimed toolkit of OECD AI Principles, UNCITRAL model laws, and international cybersecurity frameworks. Costa Rica is thus a rule-taker, not a rule-maker. It takes globally recognized norms and adapts them to its own context. Given Costa Rica's size and the source of its negotiating leverage, which comes from reputation rather than market power, that posture is fitting. What the trajectory from the CRQBIT to the CRIFTA does suggest, though, is that the gap between treaty practice and domestic ambition is closing. Slowly, unevenly, with the investment dimension still trailing. But closing.

---

[48] *Free Trade Agreement between Costa Rica and Israel* (signed 8 December 2025, not yet in force), ch 10 (Digital Trade), art 10.10, 10.18, 10.14, 10.13

[49] Ministry of Foreign Trade (COMEX), *Roadmap for Strengthening the Semiconductor Ecosystem in Costa Rica* (San José, March 2024) 56–70 (Pillar 4: Regulatory Framework - Simplification of Procedures and Facilitation of Trade and Investment.

[50] *Free Trade Agreement between Costa Rica and Israel* (signed 8 December 2025, not yet in force), ch 8

4.5. Kenya

Domestically, Kenya has a well-developed and strong digital policy framework. For instance, domestically, strategies focus on building digital infrastructure, encouraging innovation, and digital skills. Kenya has a balanced approach to data governance as it allows cross-border data flows with safeguards, but does not mandate a strict localization. However, the digital treaty commitments are still evolving in the international sphere. Kenya is also a part of multiple treaties, which show its collaborative approach regionally and globally. Participation in these agreements reflects its focus on development, growth, inclusion, and regulatory flexibility rather than opening markets without protection. Overall, Kenya maintains a strategic balance where domestic policies guide treaty practice, and international agreements help strengthen them.

A. Domestic Digital Policy Framework

Kenya is Africa's leading technology hub as it has a layered and development-driven domestic digital policy framework. It covers key sectors such as infrastructure, data protection, cybersecurity, AI, and electronic commerce. Kenya treats digitalization as central to its economic transformation. The WIR 2025 identifies Kenya as a developing country with a relatively mature digital economy framework that consistently attracts higher levels of digital FDI.[51]

The Kenya Digital Economy Blueprint (2019), developed by the Ministry of Information, Communications, and Technology, sits at the center as it defines the digital economy as the entirety of sectors that operate using digitally enabled communications and networks that leverage the internet, mobile, and other technologies. The strategy focuses on five structural pillars: Digital Government, Digital Business, Infrastructure, Innovation-driven Entrepreneurship, and Digital Skills and Values. Kenya's Vision 2030 and the Big Four Agenda also frame digitalization as a cross-cutting driver of economic growth and global integration. The framework treats privacy, data protection, and cybersecurity as enabling conditions. These conditions show that Kenya’s digital model combines market support with regulatory safeguards.

[51] United Nations Trade and Development (UNCTAD), ‘World Investment Report 2025: International Investment in the Digital Economy’ (United Nations Research Institute for Social Development 2025) <https://unctad.org/system/files/official-document/wir2025_en.pdf>.

The Kenya National Digital Master Plan 2022–2032 sets out a ten-year roadmap focusing on four main pillars: Digital Infrastructure, Digital Government Services and Data Management, Digital Skills, and Digital Innovation and Entrepreneurship and includes cross-cutting themes such as policy, legal and regulatory frameworks, research and development, data protection, and cybersecurity. The plan includes nineteen flagship programmes, including installing 100,000 km of high-speed fibre optic infrastructure, creating 25,000 internet hotspots, developing a national cloud services framework, and building 1,450 village digital hubs to attract investment. The Plan highlights the need to align ICT laws and introduce new ones to protect digital infrastructure.

The Kenya AI Strategy 2025–2030 positions AI as a tool for economic productivity and public service delivery, targeting sectors such as agriculture, health, education, and financial services, focusing on infrastructure, skills, data ecosystems, regulatory frameworks, and international cooperation.[52] The National Cybersecurity Strategy 2022–2027 is implemented through the National Computer and Cybercrimes Coordination Committee and aims to build a secure cyberspace through a coordinated approach, supporting the benefits of the digital economy.[53]

Kenya's legal framework rests on two key agreements, KICA and DPA. The KICA establishes the Communications Authority of Kenya and provides the regulatory base for the ICT sector. Part VIA of KICA addresses electronic transactions. It gives legal recognition to electronic records and validates contracts concluded electronically. Section 83G states that information cannot be denied legal effect only because it is in electronic form.[54]

The Data Protection Act ('DPA') is largely based on the EU's GDPR and gives effect to Article 31 of the Constitution of Kenya "*right not to have…information relating to their family or private affairs unnecessarily required or revealed…*". It establishes the Office of the Data Protection Commissioner as an independent enforcement authority. The DPA does not impose blanket data

[52] 'Kenya AI Strategy 2025 - 2030.Pdf' <https://ict.go.ke/sites/default/files/2025-03/Kenya%20AI%20Strategy%202025%20-%202030.pdf> accessed 24 April 2026.

[53] National Computer and Cybercrimes Coordination Committee (NC4), 'National Cybersecurity Strategy 2022 - 2027' (*National Computer and Cybercrimes Coordination Committee (NC4)*, 5 August 2022) <https://nc4.go.ke/regulations/national-cybersecurity-strategy-2022-2027/> accessed 25 April 2026.

[54] 'Kenya-Information-and-Communication-Act-1998.Pdf' <https://www.ca.go.ke/sites/default/files/CA/Statutes%20and%20Regulations/Kenya-Information-and-Communication-Act-1998.pdf> accessed 25 April 2026.

localization rules but regulates cross-border data transfers.[55] Section 48 requires data controllers to prove adequate safeguards before transferring personal data outside Kenya. Section 49 requires explicit consent for transfers of sensitive personal data. Section 50 allows the Cabinet Secretary to require that certain types of data processing take place on servers or data centres located in Kenya for reasons such as state interests or revenue protection. This creates a conditional data flow system with limited local storage requirements. It allows cross-border data flows while maintaining targeted localization and consent-based controls.

Year	Instrument	Type
2014	National Electronic Single Window System (digitising documentation)	Domestic policy
2019	Data Protection Act, No. 24 of 2019	Domestic law
2019	Kenya Digital Economy Blueprint 2019	Domestic policy
2020	Kenya–United Kingdom Economic Partnership Agreement (EPA)	Treaty
2020	Computer Misuse and Cybercrimes Act 2018 operationalised	Domestic law
2021	Data Protection (General) Regulations	Domestic regulation
2022	Kenya National Digital Master Plan 2022–2032	Domestic policy
2022	National Cybersecurity Strategy 2022–2027	Domestic policy
2023	ACP–EU Samoa Agreement (replaces Cotonou; applied Jan 2024)	Treaty
2023	AfCFTA Protocol on Investment (adopted Feb 2023)	Treaty
2023	National E-Commerce Strategy (with UNCTAD support)	Domestic policy
2023	Repeal of 30% foreign shareholding requirement for ICT companies	Domestic policy
2024	AfCFTA Digital Trade Protocol (adopted Feb 2024; pending ratification)	Treaty
2024	Kenya–EU Adequacy Dialogue launched (first in Africa)	IIA-adjacent process
2025	Kenya AI Strategy 2025–2030	Domestic policy
Ongoing	WTO JSI	Plurilateral treaty

Table 4.5.1 - Timeline of Key Domestic and Treaty Instruments

B. Treaty Practice in Digital Sphere

Kenya's treaty practice shows a developing but growing engagement with digital trade and investment. The UNCTAD IIA Navigator records digital commitments in three agreements: the ACP–EU Samoa Agreement (2023), the AfCFTA Protocol on Investment (2023) read with the AfCFTA Digital Trade Protocol (2024), and the Kenya–United Kingdom Economic Partnership Agreement (EPA) (2020). Kenya also takes part in the JSI. Kenya follows three governance

[55] 'Data-Protection-Act-1.Pdf' <https://www.kentrade.go.ke/wp-content/uploads/2022/09/Data-Protection-Act-1.pdf> accessed 25 April 2026.

models. These are development partnership, continental investment governance, and bilateral trade facilitation.

The ACP–EU Samoa Agreement was signed on 15 November 2023 and provisionally applied from 1 January 2024. It replaces the Cotonou Partnership Agreement and sets the legal and development cooperation framework between the EU and 77 OACPS members, including Kenya. The Agreement does not include a digital trade chapter, and does not set binding rules on data flows, data localization, or source code protection. It addresses digital governance through development cooperation provisions, which treat digital issues as a partnership, not a liberalization tool. They also provide the institutional and financing framework. This includes the NDICI, which has a budget of €79.5 billion for 2021–2027. This framework supports digital investment cooperation between Kenya and the EU.

The AfCFTA Protocol on Investment, adopted at the 36th African Union Summit in 2023, does not contain a dedicated digital economy chapter, but its investment facilitation provisions, which includes requirements for Parties to designate national focal points and provide information on legal, policy, and institutional frameworks governing investments, are structurally relevant to digital investors who depend on regulatory transparency and predictability.[56] The Protocol must be read alongside the AfCFTA Digital Trade Protocol (DTP), adopted at the 37th AU Assembly in 2024, which constitutes Kenya's most comprehensive multilateral digital trade instrument. The DTP addresses market access for digital products, digital trade facilitation, cross-border data flows and localization, source code protection, cybersecurity, digital inclusion, and MSME support, provisions not typically found in digital trade agreements at this level of detail.[57]

The Kenya-UK EPA, concluded in 2020 following Brexit, ensures duty-free, quota-free access for Kenyan goods to the UK.[58] The EPA does not contain a dedicated digital trade chapter, but includes a rendezvous clause providing for future negotiations on services, investment, competition policy,

---

[56] 'ACP - EU Samoa Agreement (2023) | International Investment Agreements Navigator | UNCTAD Investment Policy Hub' <https://investmentpolicy.unctad.org/international-investment-agreements/treaties/bits/5105/acp---eu-samoa-agreement-2023-> accessed 25 April 2026.

[57] 'AfCFTA Protocol on Investment (2023) | International Investment Agreements Navigator | UNCTAD Investment Policy Hub' <https://investmentpolicy.unctad.org/international-investment-agreements/treaties/tips/5114/afcfta-protocol-on-investment-2023-> accessed 25 April 2026.

[58] 'The AfCFTA Digital Protocol | International Institute for Sustainable Development' <https://www.iisd.org/articles/policy-analysis/afcfta-digital-protocol> accessed 25 April 2026.

intellectual property rights, and public procurement. In practice, the digital dimension has been developed through complementary initiatives such as the UK-Kenya Trade Logistics Information Pipeline ('TLIP'), a digital trade corridor using distributed ledger technology to support cross-border data flows. The EPA operated under the Samoa Agreement, placing the bilateral trade relationship within a broader development partnership framework.

Policy Domain	Domestic Framework	Treaty Provisions	Alignment
Data protection	DPA establishes comprehensive GDPR-modelled framework; ODPC enforces data subject rights	Samoa Agreement: development cooperation on data governance; AfCFTA DTP: data protection provisions; UK EPA: no specific data protection chapter	Aligned
Data localization	DPA: light-touch localization; one serving copy of personal data must be stored; no blanket localization mandate	AfCFTA DTP bans mandatory localization requirements by default, with public policy exceptions; UK EPA and Samoa Agreement: silent on localization	Aligned
Cross-border data flows	DPA: transfers permitted with adequate safeguards, consent, or necessity; conditional flow regime (DTI database)	AfCFTA DTP: free flow of data as default, with carve-outs for public policy and national security; JSI: disciplines on cross-border flows under negotiation	Aligned
Source code protection	Not specifically regulated domestically; no mandatory disclosure requirements	AfCFTA prohibits requiring access to source code as a market access condition, with limited exceptions for legitimate non-commercial reasons	Aligned
Electronic transactions	KICA Part VIA (ss. 83B–83S): legal recognition of electronic records, contracts, and signatures since 1998	AfCFTA DTP requires legal validity of electronic documents and contracts; UK–Kenya TLIP initiative operationalises paperless trade under the EPA framework	Aligned
E-commerce regulation	KICA s. 83C: CA mandated for e-commerce development; National E-Commerce Strategy 2023 addresses consumer protection, logistics, and trust	Samoa Agreement: e-commerce cooperation through development provisions; AfCFTA DTP: consumer protection in digital commerce; UK EPA: rendezvous clause for future e-commerce disciplines	Aligned
Digital infrastructure	Digital Master Plan 2022–2032: 100,000 km fibre, 25,000 hotspots, national cloud, 1,450 village digital hubs; calls for 2 software and 2 electronics manufacturing plants	AfCFTA Protocol on Investment Art. 17: investment facilitation for infrastructure; Samoa Agreement: NDICI funding supports digital infrastructure investment; UK EPA: goods-focused, no infrastructure chapter	Partial
AI governance	Kenya AI Strategy 2025–2030 (Ministry of ICT): pillars on infrastructure, skills, data ecosystems, regulatory frameworks, and international cooperation	AfCFTA DTP Part VII: emerging technologies and AI provisions; Samoa Agreement and UK EPA: silent on AI governance	Partial

Cybersecurity	National Cybersecurity Strategy 2022–2027 (NC4); CMCA No. 5 of 2018 establishes NC4 as the national coordination body for cybercrime prevention and response	AfCFTA DTP: cybersecurity cooperation provisions (Part V); Samoa Agreement: cybersecurity addressed through development cooperation; UK EPA: silent	Partial
Digital skills and inclusion	Digital Master Plan 2022–2032: target of 20 million digitally literate citizens; Digital Economy Blueprint: Digital Skills and Values as a core pillar	AfCFTA DTP Part VI: provisions on digital inclusion, MSMEs, entrepreneurship, and skills development; Samoa Agreement: capacity-building and technical assistance	Aligned
Investment in digital sectors	Ministry of Industry Strategic Plan 2023–2027: digital transformation as an industrial priority; 30% local shareholding requirement for ICT companies repealed in 2023	AfCFTA Protocol on Investment: post-establishment investment protection and facilitation; UK EPA: goods-focused with a rendezvous clause for investment; Samoa Agreement: development-oriented investment cooperation	Partial
Digital taxation	Finance Act 2023: 16% VAT on digital marketplace services and B2C digital sales; Digital Services Tax (1.5%) on gross digital marketplace transactions; OECD BEPS participation	AfCFTA DTP: provision on customs duties on electronic transactions; UK EPA and Samoa Agreement: silent on digital services tax	Gap
Regulatory transparency	KICA Part VI: licensing and enforcement publication requirements; Master Plan calls for harmonisation and enactment of ICT legislation	AfCFTA DTP Part IX: transparency obligations require publication of all digital-related regulations; JSI: transparency provisions for digital trade measures	Aligned

Table 4.5.2 - Domestic Digital Policy vs Treaty Provisions: Comparative Overview – Kenya

C. Domestic Law - IIA Interaction

The WIR 2025 identifies harnessing IIAs as one of four policy recommendations for investment in the digital economy, emphasising that a coherent alignment between domestic digital strategies and IIA commitments is essential for attracting and directing digital FDI toward inclusive development.[59]

The link that connects Kenya's domestic digital policies and its IIA commitments runs through data governance. Kenya's DPA (2019) establishes a conditional flow regime. This regulatory

[59] 'Kenya - United Kingdom EPA (2020) | International Investment Agreements Navigator | UNCTAD Investment Policy Hub' <https://investmentpolicy.unctad.org/international-investment-agreements/treaties/treaties-with-investment-provisions/4940/kenya---united-kingdom-epa-2020-> accessed 25 April 2026.

model enables cross-border data flows while preserving state oversight. So, the DPA does not impose a blanket localization ban which allows Kenya to engage with the AfCFTA DTP's data governance provisions. These provisions also treat data flows as a default but allow exceptions for national security and public policy reasons without requiring to reform the domestic legislation. This shows a broader pattern where domestic frameworks are already aligned with treaty disciplines; states accept those disciplines more readily and treat IIA commitments as a consolidation rather than a transformation of existing domestic law.

Kenya's statutory recognition of the legal validity of electronic transactions, anchored in Part VIA of KICA since 1998, has similarly pre-conditioned Kenya's capacity to accept treaty disciplines on digital trade facilitation. The AfCFTA DTP requires parties to recognise the legal validity of electronic documents and contracts, an obligation Kenya can fulfil without legislative reform precisely because KICA already embeds this principle.[60]

Kenya's domestic digital policies have shaped the type of IIAs it pursues. The Digital Economy Blueprint (2019) and the National Digital Master Plan (2022–2032) treat digital transformation as a development project, focusing on inclusive growth, skills, and infrastructure, not just liberalization, evident by Kenya's choice of IIA forms. Instead of negotiating advanced bilateral digital trade agreements with binding rules on data flows and source code, Kenya works through the AfCFTA and the JSI which are more cooperative and sensitive to development needs. The DTP includes rules on digital inclusion, MSME support, and capacity building. These reflect the priorities in Kenya's Master Plan and show that domestic policy has shaped the DTP's design.[61]

Kenya's digital industrial goals have also influenced the safeguards it seeks in IIAs. The National Digital Master Plan promotes local software and electronics industries. The Kenya AI Strategy 2025–2030 aims to build domestic AI infrastructure and data systems. These goals align with the AfCFTA DTP which keeps exceptions for public policy and national security in its data and source code rules to protect policy space for their digital industrial plans.

[60] Martina F Ferracane, Simón González Ugarte and Tomás Rogaler, 'Global Trends in Digital Trade Policies and Practices: Evidence from the Digital Trade Integration Database'.
[61] Georgios Dimitropoulos, 'Investment Law and the Digital Economy' (2025) 16 Journal of International Dispute Settlement idaf020 <https://doi.org/10.1093/jnlids/idaf020>.

The reverse direction, where IIA commitments shape Kenya's domestic digital policy, although less developed is becoming more important as evident from Kenya's participation in the AfCFTA DTP negotiations which includes rules on transparency and legal certainty, requiring governments to publish digital regulations and recognise electronic documents. They are already pushing domestic regulatory action. The National Digital Master Plan calls for harmonization and new ICT laws, reflecting the need to align domestic rules with regional treaty commitments.

The Kenya-EU adequacy dialogue is another important influence as the EU checks if a country's data protection system offers protection equal to EU law. This creates pressure for Kenya to improve and clarify its cross-border data transfer rules under the DPA as industry critics have commented on the rules' clarity. The pressure does not come from a binding treaty, but from the potential benefit of easier market access, showing how countries adjust their laws to match external standards even without legal obligations.

Kenya's participation in the JSI also pushes domestic reform. The JSI covers areas like electronic authentication, consumer protection, and cybersecurity. These rules require countries to build or strengthen related domestic systems. This aligns with Kenya's existing efforts, such as the National E-Commerce Strategy and the NC4 cybersecurity framework. The JSI acts as an external guide. It helps organise and reinforce Kenya's policies based on global standards.

Overall, Kenya shows a pattern of strategic compatibility. Its domestic digital policies lead its IIA choices. It joins agreements that match and support its existing system. At the same time, IIA commitments and related processes slowly shape domestic reforms. This is clear in areas like data governance and electronic transactions. This two-way relationship matches the WIR 2025 recommendation. Governments should use IIAs to signal strong and reliable regulation and attract quality digital investment, while keeping enough policy space for domestic digital growth.

4.6. Mexico

Mexico's digital policy framework is transitioning to a more export-oriented, open, and deep integration in global value chains. At the domestic end, Mexico has prioritized infrastructure, innovation, and digital inclusion, which is further reinforced through its constitutional amendments recognizing access to the internet and ICTs as a constitutional right. At the international level,

Mexico is part of some of the most advanced digital trade agreements, that includes binding commitments on cross-border data transfer and clear prohibitions on any data localization measures. Mexico adopts an open digital trade model that is significantly influenced and shaped by major digital trade agreements.

A. Domestic Digital Policies

The domestic digital policy framework in Mexico shows a gradual transition to a more structured governance model, embedded within a broader economic and industrial development strategy. Previously, the national and industrial policies in Mexico followed an import-substitution industrialization model. Nowadays, beginning in the 1980s and 1990s, Mexico evolved to a more open and export-oriented economic strategy. Mexico's integration into North American supply chains reinforces this transformation, namely through trade liberalization and agreements such as the North American FTA ('NAFTA'), which attract and encourage FDI and cross-border production networks.[62] Digital development strategies in Mexico are a combination of initiatives across sectors, constitutional reforms, and federal laws and policies.

The overall objective of Mexico's digital development strategies is to close the digital divide and enhance institutional capacity, and in recent years, national developments in Mexico have increasingly focused not just on its industrial agenda but also on its digital development agenda, namely, innovation and technological upgrading. The Programa Sectorial de Economia 2020-2024, for example, identifies innovation, competitiveness, and productivity as core pillars of Mexico's economic development strategy,[63] and, the National Digital Strategy 2021-2024 focuses on expanding broadband connectivity, digital inclusion, digitizing public services, and data transfer across the country.[64] The broader policy objectives of such developments aim to close the digital divide and support the development of a data-driven economy.

These broader policy objectives are reflected in other engagements with digital economy governance; for example, the Federal law on the Protection of Personal Data Held by Private Parties provides a national framework governing how data is collected and processed by private

[62] Jorge Carrillo and Alfredo Hualde, 'Maquiladoras in Mexico: The Export of Jobs and Technology' (1998) 4 Journal of Borderlands Studies 1.
[63] Secretaría de Economía, *Programa Sectorial de Economía 2020–2024* (Gobierno de México 2020).
[64] Gobierno de México, *Estrategia Digital Nacional 2021–2024* (2021)

entities. The Law Regulating Financial Technology Institutions ('FinTech Law') was adopted in 2018, and it regulates digital financial platforms, virtual assets, and crowdfunding services. The FinTech Law is often cited as one of the first comprehensive fintech regulatory frameworks in Latin America, and it reflects Mexico's efforts to balance innovation with regulatory oversight. More importantly, the constitutional reforms provide for the right to access information and communication technologies and broadband internet[65] and the right to personal data.[66]

B. Mexico's Treaty Practice in the Digital Sphere

The treaties in discussion in this section are the following:

(1) the United States–Mexico–Canada Agreement (USMCA);

(2) the CPTPP;
(3) the Brazil-Mexico Cooperation and Facilitation Investment Agreements ('BMCFIA');
(4) the Mexico-United Arab Emirates Bilateral Investment Treaty ('MUAEBIT').

Mexico is party to several major trade agreements with digital trade and data governance provisions. Its treaty practice demonstrates a robust integration into regional and global economic governance frameworks. The USMCA, for example, includes a comprehensive and dedicated digital trade chapter that promotes cross-border data flows, protects proprietary source code from forced disclosure, and prohibits data localization requirements for computing facilities.[67] Chapter 19 of the USMCA is one of the most advanced digital trade frameworks currently in force, placing Mexico within this highly integrated North American digital economy. In parallel, the CPTPP also provides provisions governing electronic commerce, cross-border data flows and transfers between member states, as well as digital authentication.[68]

However, as observed, Mexico's BIT practice remains more traditional. For example, the BMCFIA mainly focuses on investment facilitation mechanisms, other transparency obligations,

---

[65] CPEUM, art 6 (as amended by Decreto de Reforma Constitucional en Materia de Telecomunicaciones, DOF 11 June 2013).
[66] CPEUM, art 16 (as amended, DOF 1 June 2009).
[67] *USMCA* (signed 30 November 2018, entered into force 1 July 2020) ch 19 (Digital Trade).
[68] *Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) (entered into force for Mexico 30 December 2018)*
<https://www.mscbs.gob.es/profesionales/saludPublica/ccayes/alertasActual/Docs/cptpp_eng.pdf>

and cooperation rather than addressing digital governance obligations in detail. The same applies to other agreements, for example, the MUAEBIT, which largely follows traditional investment treaty structures, with limited explicit references to the digital economy or digital governance.

C. Domestic Law – IIA Interaction

Mexico's domestic digital policy and treaty practices appear broadly complementary on the surface; however, they are mostly shaped by the country's integration into regional economic agreements. As seen above, Mexico has developed a domestic regulatory environment that encourages and supports innovation in the digital sphere, cybersecurity and data protection governance, and fintech development, while maintaining regulatory oversight. This national strategy aligns with its treaty obligations by encouraging cross-border data transfers and digital trade. Furthermore, Mexico's strategy of integrating into the global digital value chain and maintaining its regulatory compatibility with major trade partners is evident in its participation in agreements such as USMCA and CPTPP.

This suggests that the direction of influence is operating mainly from international agreements to domestic policy development. Many of the initiatives developed and implemented domestically are broadly consistent with the open digital trade model found in the country's major regional economic agreements. The USMCA and the CPTPP provide clear commitments and rules that facilitate cross-border digital commerce; for example, the USMCA digital chapter does not allow data localization measures. Broadly speaking, Mexico's domestic digital policies are in line with this model as it adopted a national data protection law, which does not impose strict data localization measures. The FinTech Law also regulates financial services platforms and does not impose strong restrictions on cross-border transactions.

Rather than emerging independently as a distinct national regulatory model, Mexico's digital policy frameworks have evolved within the context of its broader economic integration, and do not appear to be exporting a unique digital governance model through its treaties. It is clear from the developments and constitutional reforms in recent years that Mexico's domestic policies increasingly reflect the models, regulatory standards, and disciplines found in the regional agreements to which it is a party.[69]

[69] See Gobierno de México, Estrategia Digital Nacional 2021–2024 (2021).

4.7. Nigeria

Domestically, Nigeria has a strong and development-focused digital policy. It is led by NDEPS 2020-2030, which focuses on infrastructure, improving digital skills, and supporting local businesses. The government also uses laws to encourage innovation and protect data and allows for cross-border data flows without strict localization. It also strengthened its digital systems through projects like eNaira and 5G. However, Nigeria lags in terms of international digital agreements as older treaties do not cover digital issues well and rely more on regional and global platforms like AfCFTA. Overall, Nigeria shows strong domestic leadership but slower treaty progress and tries to attract investment while protecting its own interests.

A. Domestic Digital Policy Framework

Nigeria has a layered development-oriented domestic digital policy framework. Assessed against the WIR 2025 criteria and its accompanying Toolkit for Policymakers, the framework of Nigeria has characteristics of economies that consistently attract higher levels of digital FDIs.

The *National Digital Economy Policy and Strategy 2020-2030* ('NDEPS') lies at the center of Nigeria's digital architecture and constitutes the core instrument of its digital architecture. The policy is organised around eight pillars: Developmental Regulation, Digital Literacy and Skills, Solid Infrastructure, Service Infrastructure, Digital Services Development and Promotion, Soft Infrastructure, Digital Society and Emerging Technologies, and Indigenous Content Development and Adoption.[70] The NDEPS is explicitly state-directed and developmentally oriented: Pillar 8 prioritises local digital capability development, and Pillar 3 frames connectivity infrastructure as a prerequisite for economic participation. Pillar 1, Developmental Regulation, reflects Nigeria's approach of regulating the digital economy not as a constraint on market actors but as a developmental tool, using regulation to shape digital markets while maximising domestic value capture.[71]

[70] Justice Tei Mensah and Nouhoum Traore, 'Infrastructure Quality and FDI Inflows'.
[71] 'National-Digital-Economy-Policy-and-Strategy.Pdf' <https://nitda.gov.ng/wp-content/uploads/2020/06/National-Digital-Economy-Policy-and-Strategy.pdf> accessed 25 April 2026.

The Nigeria Startup Act 2022 operationalises the NDEPS by providing a dedicated legal framework for the technology startup ecosystem, including a Seed Fund, simplified regulatory access for fintech startups, intellectual property protections, and a requirement that at least one-third of a labelled startup's local shareholding be held by Nigerians.[72] The Nigeria Data Protection Act 2023 (NDPA) establishes the independent Nigeria Data Protection Commission (NDPC). It creates a standards-based cross-border data governance regime, allowing conditional data transfers based on adequacy decisions or contractual safeguards and not imposing blanket data localization requirements.[73] The NDPA aims to strengthen the legal foundation of the national digital economy. It also aims to ensure Nigeria's participation in regional and global economies through the trusted use of personal data. This language shows a clear link between domestic data governance and international economic integration.[74]

The CBN Payment System Vision 2025 and its successor PSV 2028 provide the financial infrastructure layer. They include the eNaira central bank digital currency, the AfriGo domestic card scheme, and an Open Banking regulatory framework.[75] The National Policy on 5G (2023) completes the infrastructure dimension. It presents fifth-generation connectivity as essential for advanced digital economy uses such as smart infrastructure, and Industry 4.0 manufacturing.[76]

Year	Instrument	Type
2016	Nigeria–Singapore Bilateral Investment Treaty	Treaty
2020	National Digital Economy Policy and Strategy (NDEPS)	Domestic policy
2021	National Digital Innovation &Entrepreneurship Policy (NDIESP)	Domestic policy
2022	CBN Payment System Management & Vision	Domestic policy
2022	Nigeria Startup Act	Domestic law
2023	National Policy on 5G Networks (Decree No. — FMCIDE)	Domestic policy

[72] 'NIGERIA-STARTUP-ACT-2022' <https://placng.org/i/wp-content/uploads/2023/01/NIGERIA-STARTUP-ACT-2022.pdf> accessed 25 April 2026.
[73] Nigeria Data Protection Act 2023, No 37, ss 1, 41–43 <https://ndpc.gov.ng/wp-content/uploads/2024/03/Nigeria_Data_Protection_Act_2023.pdf> accessed 16 March 2026.
[74] 'PSV2025 | Central Bank of Nigeria' <https://www.cbn.gov.ng/PaymentsSystem/PSV2025.html> accessed 25 April 2026.
[75] 'National Policy on Fifth Generation (5G) Networks for Nigeria's Digital Economy'.
[76] 'Nigeria - Singapore BIT (2016) | International Investment Agreements Navigator | UNCTAD Investment Policy Hub' <https://investmentpolicy.unctad.org/international-investment-agreements/treaties/bilateral-investment-treaties/3705/nigeria---singapore-bit-2016-> accessed 25 April 2026.

2023	Nigeria Data Protection Act (NDPA)	Domestic law

Table 4.7.1 - Timeline of Key Domestic and Treaty Instruments

B. Treaty Practice in the Digital Sphere

Nigeria's treaty practice in the digital sphere shows a structural split. One group includes traditional BITs that came before digital trade rules. The other includes newer multilateral and continental instruments that address digital trade more directly but have not fully entered into force. Nigeria does not yet have a dedicated bilateral digital trade agreement. The most relevant agreements in the past five years include the Nigeria–Singapore BIT (2016), the AfCFTA Digital Trade Protocol (2024), and Nigeria's participation in the JSI.

The Nigeria–Singapore BIT, signed on 4 November 2016, is not yet in force. It is a traditional investment protection agreement.[77] It does not include digital-specific provisions like cross-border data flows, source code protection, or limits on data localization. It uses a broad, asset-based definition of "investment," which covers investments in digital infrastructure and technology platforms. The UNCTAD IIA Mapping Project notes that the BIT includes general public policy exceptions. These exceptions may allow some regulatory space for digital economy measures. However, they are broad and not designed specifically for digital governance.[78]

The AfCFTA DTP, adopted in February 2024, is the most advanced digital trade instrument to which Nigeria is a party, addressing cross-border data transfers, source code disclosure, digital identities, financial technology, cybersecurity, and online consumer protection, with eight annexes still under negotiation.[79] Nigeria's designation as AU Digital Trade Champion reflects the country's substantive engagement in shaping the DTP's content, a dynamic in which domestic policy maturity translates into negotiating leverage at the international level. Nigeria's participation in the JSI further extends its multilateral digital trade engagement.

Policy Domain	**Domestic Framework**	**Treaty Provisions**	**Alignment**

[77] 'Nigeria - Singapore BIT (2016) | International Investment Agreements Navigator | UNCTAD Investment Policy Hub'<https://investmentpolicy.unctad.org/international-investment-agreements/treaties/bilateral-investment-treaties/3705/nigeria---singapore-bit-2016-> accessed 25 April 2026.
[78] 'The AfCFTA Digital Protocol | International Institute for Sustainable Development' <https://www.iisd.org/articles/policy-analysis/afcfta-digital-protocol> accessed 25 April 2026.
[79] Georgios Dimitropoulos, 'Industrial Policy and the New Internationalism'.

Data protection	NDPA 2023 regulates data processing, rights & NDPC oversight	Nigeria–Singapore BIT: investor data protection provisions (Art. 9)	Aligned
Data localization	NDPA permits cross-border transfers; no blanket localization mandate	BIT silent on localization requirements; no explicit prohibition	Partial
Cross-border data flows	NDPA allows with adequate safeguards; NDEPS promotes digital trade openness	BIT guarantees free transfer of capital and returns (Arts. 7–8)	Aligned
E-commerce regulation	NDEPS and Startup Act 2022 support digital commerce; no standalone e-commerce law	BIT limited to investment protection; no specific e-commerce provisions	Gap
Digital infrastructure	National 5G Policy (2023) and NDEPS promote ICT infrastructure rollout	BIT protects infrastructure investment; no specific digital infrastructure clause	Partial
Payment systems	CBN Payment System Vision 2025 governs digital payments and fintech	BIT guarantees free transfer of returns; no fintech-specific provisions	Partial
Startup & innovation	Startup Act 2022 and NDIESP provide legal labelling, incentives & support	BIT protects investors broadly; no startup-specific investment facilitation chapter	Partial
AI governance	NDIESP mentions emerging tech; no dedicated AI regulatory framework	No AI references in the Nigeria–Singapore BIT 2016; limited treaty references	Gap
Source code & IP	Startup Act recognises IP; source code not strongly regulated domestically	BIT includes IP as covered investment; no source code protection provisions	Partial

Table 4.7.2 - Domestic Digital Policy vs Treaty Provisions: Comparative Overview

C. Domestic Law - IIA Interaction

Although the relationship between Nigeria's domestic digital policies and its IIAs is asymmetric, it still works in both directions. The domestic framework is more advanced than the treaty portfolio, and the links operate differently depending on the direction. This asymmetry is important. As WIR 2025 notes, countries with mature digital economy policies attract more digital FDIs, but only when the treaties clearly signal regulatory stability to foreign investors.[80]

An example of domestic digital policy shaping treaty commitments is Nigeria's data governance model. The NDPA 2023 uses a standards-based, rights-oriented approach and does not impose blanket data localization requirements. Instead, it allows cross-border transfers based on adequacy or contractual safeguards which directly sets the limits for Nigeria's treaty commitments on data

[80] United Nations Trade and Development (UNCTAD), 'World Investment Report 2025: International Investment in the Digital Economy' (United Nations Research Institute for Social Development 2025) <https://unctad.org/system/files/official-document/wir2025_en.pdf>.

flows. Because the NDPA does not require localization, Nigeria can accept open cross-border data flow rules in the DTP and the JSI without conflict with its domestic law. Simultaneously, the NDPC retains discretion to decide adequacy and issue compliance guidance, preserving regulatory autonomy and protecting against broad treaty constraints.[81]

Second, the Startup Act's local shareholding requirement and the NDEPS Indigenous Content Pillar show a domestic preference for local digital ownership. Nigeria's BITs do not replicate these preferences in treaty form, but these domestic commitments act as a floor below which Nigeria is unlikely to accept liberalization commitments in future treaty negotiations. The DTI Database indicators for Nigeria on FDI in digital trade-related sectors and commercial presence requirements for digital services providers reflect this residual protectionist preference.[82]

Third, and most significantly, Nigeria's domestic experience as a rule-maker in digital payments, including the eNaira, AfriGo, and the National Payment Stack, has translated into treaty-shaping capacity in the DTP negotiations. Nigeria's designation as AU Digital Trade Champion reflects a dynamic where domestic policy maturity creates negotiating leverage internationally, aligning with WIR 2025 Toolkit's observation that countries with more mature digital economy frameworks are better able to shape multilateral rules rather than simply adopt them.[83]

The reverse link, treaty provisions shaping domestic policy, is still more latent than active in Nigeria as neither the Nigeria-Singapore BIT nor the Nigeria-Morocco BIT has come into force. However, anticipatory alignment is already visible. The NDPA 2023 cross-border transfer regime and the NDPC mandate to participate in international forums are designed to ensure Nigeria's compatibility with future treaty obligations under the AfCFTA DTP and the JSI, both of which include data flow disciplines. The NDPA adopts an adequacy-based model similar to the EU

[81] 'National-Digital-Economy-Policy-and-Strategy.Pdf' <https://nitda.gov.ng/wp-content/uploads/2020/06/National-Digital-Economy-Policy-and-Strategy.pdf> accessed 25 April 2026. Pillar 8.

[82] United Nations Conference on Trade and Development, *World Investment Report 2023: Investing in Sustainable Energy for All* (UNCTAD 2023) 142–146; UNCTAD, *Digital Trade and Investment (DTI) Database-Nigeria Economy Profile* (2024) https://investmentpolicy.unctad.org/dti accessed 13 April 2026.

[83] United Nations Conference on Trade and Development, *World Investment Report 2025: International Investment Governance and the Digital Economy (Toolkit)* (UNCTAD 2025) 58-63; UNCTAD, *World Investment Report 2021: Investing in Sustainable Recovery* (UNCTAD 2021) 174–178 https://unctad.org/publication/world-investment-report-2021 accessed 13 April 2026.

GDPR and reflects the approach used in modern digital trade agreements and signals an intent to align with emerging international norms embedded in treaty form.

Nigeria's participation in the AfCFTA DTP negotiations creates a feedback loop between treaty negotiation and domestic policy reform. The ongoing negotiation of the Protocol's annexes on digital payments, fintech, and source code disclosure generates. It pressures and provides a reference point for the Central Bank of Nigeria and relevant ministries to align their domestic regulatory frameworks prior to the protocol's entry into force. Nigeria's anticipatory alignment in data governance and payments regulation reflects an awareness that treaty commitments, including prospective ones, can function as commitment devices to attract digital investment.

Overall, Nigeria's domestic treaty interaction is characterised by leadership in domestic policy but a lag in treaty practice. While the BITs are not yet in force and do not contain digital-specific provisions, the domestic framework is sophisticated and oriented toward integrating international digital trade norms. The gap between domestic policies and treaty practice is being addressed through multilateral channels (the DTP and the JSI) rather than through bilateral digital trade agreements. Nigeria's context-sensitive treaty practice accepts deeper digital commitments within the DTP framework but defers bilateral digital disciplines. This approach reflects a deliberate strategy to preserve domestic policy space while building credibility internationally.[84]

4.8. Pakistan

Pakistan's domestic digital policy and treaty practices stand disconnected. On one side, Pakistan has developed its domestic digital policy through e-commerce legislation, national cyber security framework and cloud governance policies, indicating its ambition on paper to develop a digital economy, while on the other side, their BIT's are Pakistan-Türkiye Trade in Goods Agreement (2022) and the Pakistan-Bahrain BIT (2014) is completely silent on digital trade, data governance or cyber security. None of the domestic digital policies has paved its way into international agreements. The relationship of the domestic-treaty defines disengagement as Pakistan's treaties impose no digitally enhanced provisions or chapters, and its domestic regulatory development,

[84] United Nations Trade and Development (UNCTAD), 'World Investment Report 2025: International Investment in the Digital Economy' (United Nations Research Institute for Social Development 2025) <https://unctad.org/system/files/official-document/wir2025_en.pdf>.

which remains largely unimplemented and fragmented, with no influence of any of its international treaty anchors.

A. Domestic Digital Policies

While Pakistan acknowledges the digital economy as central to its developmental strategy, it still lacks the proper legal and regulatory framework to centralize this in its domestic digital policy. The Pakistan Vision 2025 operates as the overarching objective in this space through the Digital Pakistan Policy 2018, which emphasizes digital infrastructure and economic transformation.[85] The Digital Policy 2018 promotes e-commerce, digitizing public services, and increasing investing in the tech sector.[86] The Cloud First Policy is an example of a more recent digital policy measure that directs the public sector to adopt cloud-based solutions.[87] It is also worth noting that these national directives are then adopted on a provincial level, such as in Gilgit-Baltistan.[88]

At the legislative level, the Electronic Transactions Ordinance 2002 provides the foundational legal basis for e-commerce by recognising electronic documents and signatures as legally valid.[89] On the other hand, the National Cyber Security Policy 2021, which is Pakistan's first comprehensive national framework in this area, establishes governance structures for cybersecurity, including a Cyber Governance Policy Committee. It calls for engagement with international bodies such as the ITU, ICANN, and other regional organizations.[90]

Additionally, Pakistan also introduced the Personal Data Protection Act last year, which regulates cross-border data transfer and the processing of personal data.[91] These measures collectively show us that while Pakistan is on the cusp of implementing domestic measures, they are still in the

---

[85] Planning Commission of Pakistan, Pakistan Vision 2025 (Government of Pakistan 2014).
[86] Ministry of Information Technology and Telecommunication, Digital Pakistan Policy (Government of Pakistan, 22 May 2018).
[87] Ministry of Information Technology and Telecommunication, Pakistan Cloud First Policy (Government of Pakistan 2022).
[88] Government of Gilgit-Baltistan, Gilgit-Baltistan Cloud First Policy 2024 (GBIT 2024).
[89] Electronic Transactions Ordinance 2002 (Pakistan), s 3.
[90] Ministry of Information Technology and Telecommunication, National Cyber Security Policy 2021 (Government of Pakistan, July 2021).
[91] Personal Data Protection Bill 2023 (Pakistan), cls 13 <https://moitt.gov.pk/SiteImage/Misc/files/Final%20Draft%20Personal%20Data%20Protection%20Bill%20May%202023.pdf> accessed 11 March 2026

elementary phase. For example, there is no known blanket data localization policy for private entities. The majority of the regulations are sector-specific and provide no overarching policy.

Year	Instrument	Type
2002	Electronic Transactions Ordinance 2002	Domestic law
2014	Pakistan–Bahrain Bilateral Investment Treaty	Treaty
2018	Digital Pakistan Policy	Domestic policy
2021	National Cyber Security Policy 2021	Domestic policy
2022	Pakistan Cloud First Policy	Domestic policy
2022	Pakistan–Türkiye Trade in Goods Agreement	Treaty
2022	Pakistan–Uzbekistan Preferential Trade Agreement	Treaty
2024	Gilgit-Baltistan Cloud First Policy 2024	Domestic policy
2025	Personal Data Protection Bill 2025	Draft legislation
Ongoing	WTO JSI on Electronic Commerce (non-participant)	Plurilateral

Table 4.8.1 Timeline of Key Domestic and Treaty Instruments

B. Treaty Practice in the Digital Sphere

The treaties in discussion in this section are the following:

(1) the Pakistan–Türkiye Trade in Goods Agreement (‘TIG Agreement’);
(2) the Agreement between the Government of the Islamic Republic of Pakistan and the Government of the Kingdom of Bahrain on the Promotion and Protection of Investments (‘PBPPI’); and
(3) the Pakistan-Uzbekistan Preferential Trade Agreement (‘PUPTA’).

Pakistan's bilateral treaty practice does not engage with the digital economy. The Pakistan-Türkiye Trade in Goods Agreement 2022 and the Pakistan-Bahrain BIT 2014 follow pre-digital templates and are wholly silent on digital trade, data governance, and digital investment facilitation. The most that can be said is that the TIG Agreement references cooperation on computerised customs systems in passing[92] and requires trade-related laws to be available online where feasible,[93] while the PBPPI implicitly covers digital intellectual property assets through its broad investment

[92]Trade in Goods Agreement between the Government of Islamic Republic of Pakistan and the Government of Türkiye (signed in 2022, enforced in 2023) ('PAK-TUR TIG') art 14(1).
[93]Ibid art 16(1).

definition[94] and provides binding ICSID arbitration.[95] Neither agreement contains provisions on cross-border data flows, data localization, source code protection, cybersecurity, electronic authorizations, or digital capacity building.

Even for the most recently introduced legislation, these key issues persist. For example, the PUPTA in 2022 only focuses on tariffs and transparency obligations and has no digital dimension at all.[96] Agreements that are established before 2022 also remain entirely free of any digital dimension. This shows that Pakistan has a consistent pattern in its treaty practices because the digital economy has simply not been featured as a subject in bilateral negotiations.

This positioning extends to the multilateral level. Pakistan is one of only twelve WTO members that did not participate in any WTO plurilaterally, including the JSI.[97] At the WTO General Council meeting of February 2025, Pakistan did not support the proposal to formalise the concluded Agreement on Electronic Commerce by annexing it to WTO rules under Annex 4, even though this procedure requires consensus. Compounding this with Pakistan's bilateral treaty practices, it shows that the absence of digital trade commitments is not incidental but reflects a consistent and deliberate posture across both bilateral and multilateral engagement.

Policy Domain	Domestic Framework	Treaty Provisions	Alignment
Data protection	Personal Data Protection Bill (2025 draft) regulates collection, processing and cross-border transfer of personal data	No treaty provisions on data protection in mapped agreements	Gap
Data localization	No explicit statutory data localization mandate identified	No treaty restriction or prohibition on localization	Not engaged
Cross-border data flows	Allowed with safeguards	No treaty provisions on data flows	Gap
E-signatures	Electronic Transactions Ordinance 2002	PAK-TUR TIG Art 16: online publication of laws 'where feasible'; no e-signature provision	Partial

[94] Agreement between the Government of the Islamic Republic of Pakistan and the Government of the Kingdom of Bahrain for the Promotion and Protection of Investments (signed 2014, not yet in force) ('PAK-BHR BIT') art 1(1)(d).

[95] Ibid art 9.

[96] Preferential Trade Agreement between the Government of the Republic of Uzbekistan and the Government of the Islamic Republic of Pakistan (signed 3 March 2022, entered into force 2022) ('PAK-UZB PTA') arts 1-18.

[97] Peter Ungphakorn, 'E-Commerce Initiative is the Latest WTO Rule-Making Effort to be Blocked' (Trade Beta Blog, 19 February 2025, updated 7 December 2025) <https://tradebetablog.wordpress.com/2025/02/19/e-commerce-initiative-latest-blocked> accessed 11 March 2026.

E-commerce	ETO 2002, Digital Pakistan Policy promotes e-commerce.	No e-commerce chapter or provisions	Gap
Digital infrastructure	Strong domestic policy	No treaty reflection	Gap
AI governance	No dedicated AI law or policy	No treaty provisions on AI	Not engaged
Cybersecurity	National Cyber Security Policy 2021	No cybersecurity provisions	Gap

Table 4.8.2 - Domestic Digital Policy vs Treaty Provisions: Comparative Overview

C. Domestic Law – IIA Interaction

One might argue that the pattern of the lack of digital infrastructure in both domestic and international treaties signals structural disengagement. Unlike countries such as Mexico, where high-ambition regional agreements have shaped domestic regulatory choices, Pakistan's treaties impose no digital disciplines and exert no influence over its domestic policy trajectory. The agreements do not mention all key digital economy parameters, leaving Pakistan with full regulatory autonomy in these areas. The issue of the digital economy has not arisen in the treaty context at all.

The direction of influence does not run clearly in either direction. Pakistan's domestic instruments reflect genuine national regulatory priorities. However, none of these have been translated into treaty commitments or cooperative mechanisms. The Cyber Security Policy, for example, calls for Pakistan to maintain a presence in international bodies such as the ITU, ICANN, and APT. It also pushes to develop trusted information-sharing mechanisms on cyber threats with governmental and non-governmental bodies globally.[98] However, no such cooperative framework appears in any of the mapped bilateral agreements. Pakistan has neither used its treaties to export its regulatory approach nor been subjected to treaty guidelines that would constrain it. The domestic agenda and treaty practice remain unlinked from each other without any substantive connection.

This disconnect creates a latent tension. The Personal Data Protection Bill 2023 cross-border transfer provisions point toward a domestic regulatory direction that values oversight of data governance. Should Pakistan enter future digital trade agreements incorporating standard disciplines such as prohibitions on data localization, now common in modern digital trade chapters,

[98] Ministry of Information Technology and Telecommunication, National Cyber Security Policy 2021 (Government of Pakistan, July 2021) s 3.11.

these domestic instruments could come under treaty pressure. This tension remains latent for now, but it points to a gap in strategic coherence between Pakistan's domestic regulatory direction and its treaty-making practice that will need to be addressed as its international economic engagements deepen.

4.9. Peru

The commitments embedded in Peru's FTAs incorporate substantial provisions on digital trade. Domestically, Peru has established a solid digital policy framework, setting in motion a programme to modernise public administration, expand broadband access nationwide, and open up avenues for growth and inclusion in the digital economy. Peru is also a co-sponsor of several JSI papers on electronic commerce. In addition, the country's laws govern cross-border data transfers, permitting them to jurisdictions or international organizations that provide an adequate level of data protection. That said, Peru's regulatory framework for the digital economy is still at an early stage. Even so, recent legislative developments point to a clear and deliberate effort to position the country for deeper integration into global digital value chains going forward.

A. Domestic Digital Policies

Peru's digital policy is carried out by the public sector at the national level to promote the development of information technologies and to achieve the productive transformation of the economy and an efficient public administration, and also to strengthen the regulatory State in the area of data protection, e-commerce, and the digital infrastructure. Domestic digital policy in Peru is currently undergoing quick development within the last ten years.

The main policy instrument at the national level is the National Digital Transformation Policy adopted in 2020, which intends to modernise digital infrastructure through the implementation of online public services and the widespread use of digital technologies. It also looks to the future of digital innovation and possible opportunities to increase the productivity of the economy and to strengthen Peru's participation in global digital value chains.[99]

[99] Government of Peru, *Política Nacional de Transformación Digital* (Peru, 2020). (Original document in Spanish, English translation AI assisted.)

Similarly, the Digital Government Framework Law aims at transforming the public administration through digital technologies. This law has a triple focus: first, on the provision of digital public services; second, on the interoperability within the public administration; and, finally, on the use of digital channels to ensure the modernization of public administration, increasing the efficiency, transparency, accountability, and innovation of public activities. Strengthening digital governance in Peru is crucial for the consolidation of a Digital State.[100]

In Peru, personal data protection is regulated by Law No. 29733, Personal Data Protection Law, which establishes that the Law will regulate the collection, processing, and transfer of personal data. This Law deals with the processing of personal information by public or private entities and data protection measures, such as safety and confidentiality. The cross-border transfer of personal data is allowed when there are appropriate safeguards. In this way, the Peruvian law aims to balance the protection of privacy and the development of electronic commerce.[101]

There are also specific national initiatives for developing broadband and digital inclusion to reduce the digital divide. The recent initiatives confirm that the digital infrastructure is an important factor in Peru's economic development and its entry to the digital economy.[102]

The Peruvian digital policy for the internal market is developing institutionally and regulatoryally. The digital governance framework in Peru is in a lower development stage compared to advanced countries; therefore, the recent measures are a large step in improving the regulations on the digital economy, digital infrastructure, and the development of the ICT sector.

Peru's institutional capacity in cybersecurity is anchored by PECERT (i.e., Computer Emergency Response Team) which serves as the national point of contact for responding to cyber incidents. This function is directly relevant to the cybersecurity cooperation obligations that now feature as standard provisions in Peru's most recent FTAs, including the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (Art. 14.16) and the Hong Kong–Peru FTA (Art.

[100] Congress of the Republic of Peru, Ley de Gobierno Digital (Legislative Decree No 1412) (Peru, 2018). (Original document in Spanish, English translation AI assisted.)

[101] Congress of the Republic of Peru, Ley de Protección de Datos Personales No 29733 (Peru, 2011) and Supreme Decree No 003-2013-JUS approving the Regulation of the Personal Data Protection Law (Peru, 2013). (Original documents in Spanish, English translation AI assisted.)

[102] Ministry of Transport and Communications (Peru), Plan Nacional de Banda Ancha y Estrategia de Conectividad Digital (Peru, 2019). (Original document in Spanish, English translation AI assisted.)

11.17(2)). These provisions call on parties to strengthen the capabilities of national entities responsible for computer security incident response and to leverage existing cooperation mechanisms to detect and address malicious intrusions. Within this framework, PECERT should be recognised as the institutional anchor through which Peru operationalises and fulfils these commitments.

Instrument	Year	Primary Focus	Relevance to Digital Trade
National Digital Transformation Policy	2020	Digital infrastructure; online public services; digital innovation	Aligns with cooperation provisions in FTA digital chapters
Digital Government Framework Law	2018	Digital public services; interoperability; e-government	Supports paperless trading obligations (e.g., HK-Peru FTA Art. 11.13)
Personal Data Protection Law (Law No. 29733)	2011	Collection, processing, and transfer of personal data	Directly relevant to cross-border data flow obligations in CPTPP Art. 14.11 and HK-Peru FTA Art. 11.10
Broadband & Digital Inclusion Initiatives	Ongoing	Reducing the digital divide; expanding connectivity	Background condition for effective implementation of e-commerce commitments
PECERT (Cybersecurity Response Team)	Operational	National cybersecurity incident response	Relevant to CPTPP Art. 14.16 and HK-Peru FTA Art. 11.17 cybersecurity cooperation obligations

Table 4.9.1 Domestic law alignment with digital trade obligations

B. Treaty Practice in the Digital Sphere

The treaties that will be discussed in this section are the following:

(1) The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP);
(2) the United States-Peru Trade Promotion Agreement (PTPA);
(3) The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP);
(4) The United States-Peru Trade Promotion Agreement (PTPA);
(5) The Hong Kong, China–Peru Free Trade Agreement (HK-Peru FTA, 2024); and
(6) The Pacific Alliance–Singapore Free Trade Agreement (PA-Singapore FTA, 2022).

As is becoming standard practice, Peru's digital trade commitments are included so far in the electronic commerce or digital trade chapters of its FTAs. Peru has a robust set of treaties with digital trade provisions, in addition to coverage in the CPTPP and the US-Peru Trade Promotion

Agreement, discussed below. Peru's FTAs with Hong Kong, China (2024) and with the Pacific Alliance member countries jointly with Singapore (2022) contain detailed chapters on e-commerce, reviewed in this section. Peru is a co-sponsor of the WTO Joint Statement Initiative on Electronic Commerce. These agreements provide for measures to facilitate digital trade, promote electronic commerce, and achieve regulatory cooperation.[103]

As discovered, the CPTPP is one of the most significant agreements for digital trade for Peru. It contains a specific electronic commerce chapter dealing with issues such as cross-border data flows, data localization restrictions, electronic authentication, and others. For instance, Article 14.11 of the CPTPP states 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."*

This provision reflects a broader trend in modern trade agreements favouring the free flow of data across borders as a key component of digital trade. The CPTPP also addresses data localization requirements and limits its use. Article 14.13 of the agreement states:

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

While CPTPP commits contracting parties to address issues such as the free flow of data, and data localization, the Agreement includes two other provisions that are typical in Peru's FTAs. Article 14.4 on non-discrimination of digital products is more stringent than the best-endeavours commitment found in the HK-Peru FTA (Art. 11.9). Article 14.17 requires that mass-market software not be subject to requirements for transfer of or access to source code as a condition on importation or distribution, sale (including e-commerce), or use within the party's territory. Article 14.16 requires the Committing Parties to develop capabilities to respond to any potential cyber incident, as well as to cooperate for early detection and addressing of cyber incursions.

Moreover, Peru has begun negotiating additional digital trade terms in its other bilateral FTAs. Additionally, the PTPA, signed in 2007 and entered into force in 2009, established a

[103] Mira Burri, María Vásquez Callo-Müller and Kati Kugler, 'The Evolution of Digital Trade Law: Insights from TAPED' (2024) 23(2) *World Trade Review* 190, 191.

comprehensive FTAs between the two countries and includes provisions dealing with e-commerce and the facilitation of digital trade. These reflect the increasing importance of e-commerce and seek to promote collaboration in areas such as electronic authentication, consumer protection, and other areas of paperless commerce.[104]

The Hong Kong, China–Peru FTA, entered into force in 2024, has very comprehensive digital trade provisions, concentrated in Chapter 11 on Electronic Commerce. Article 11.10 on cross-border data flows, follows the same mandatory language and spirit as found in the CPTPP but also includes an important carve-out to ensure that legitimate public policy objectives are not unduly hindered by restrictions, and that such restrictions are not applied in an arbitrary or discriminatory manner for protection of domestic industry. Article 11.11 on data localization mirrors the CPTPP language in prohibiting parties from enforcing measures that require the use of servers or data centres located within their territories for the storage or processing of data. Article 11.9 on national treatment of digital products departs from the CPTPP language, which commits parties to best-endeavours to ensure national treatment for digital products. Article 11.16 on source code replicates the CPTPP prohibition. Article 11.12 on personal data protection requires each party to ensure that it has in place a legal framework to protect personal information, and to take into account relevant international principles and guidelines when enforcing its laws. Article 11.17 on cybersecurity requires parties to build domestic capabilities to respond to cybersecurity incidents, and to cooperate to identify and address the source of malicious intrusions. The chapter also addresses issues of paperless trading (Art. 11.13), internet access principles (Art. 11.14), and unsolicited commercial electronic messages (Art. 11.15).

Peru is a Pacific Alliance member, and hence a signatory to the PA-Singapore FTA, signed in 2022. Chapter 13 on digital trade follows the CPTPP model. The cooperation article (Art. 13.16) promotes cross-border information exchange and specifically requires the promotion of access for persons with disabilities to Information and Communication Technology. A Services, Investment and E-Commerce Committee (Article 13.19) is in charge of the digital chapter, and Peru can count on this institutional mechanism within the Pacific Alliance framework.

[104] Government of the United States and Government of Peru, United States-Peru Trade Promotion Agreement (Washington/Lima, 2007, entered into force 2009), ch 15 (Electronic Commerce).

The multilateral element involves Peru's participation in the JSI. Peru is one of the co-sponsors of the plurilateral group of JSI partners pursuing disciplines on digital trade across several issues, including customs duties on electronic transmissions, electronic authentication methods, consumer protection, data flows, data localization requirements, and source code protection. The disciplines in the JSI initiative substantially overlap with many of the bilateral commitments that Peru has in its trade agreements. Article 11.3 of the HK-Peru FTA commits the two parties to review the results of WTO e-commerce negotiations once those negotiations enter into force.

Overall, Peru's treaty practice demonstrates a commitment to facilitating digital trade while maintaining flexibility for domestic regulation. By incorporating digital trade provisions into its trade agreements, Peru seeks to promote cross-border digital commerce and enhance its integration into the global digital economy.

Discipline	**CPTPP**	**HK-Peru FTA (2024)**	**PA-Singapore (2022)**	**PTPA (2009)**
Customs duties on e-transmissions	Binding	Binding	Binding	Binding
Non-discrimination of digital products	Binding	Best endeavours	Binding	Binding
Cross-border data flows	Binding	Binding (+ policy carve-out)	Binding	Partial
Data localization prohibition	Binding	Binding	Binding	Not explicit
Electronic authentication	Binding	Binding	Binding	Binding
Consumer protection (e-commerce)	Binding	Binding	Binding	Binding
Personal data protection framework	Best endeavours	Binding	Best endeavours	Limited
Spam / unsolicited messages	Binding	Binding	Binding	Binding
Paperless trading	Best endeavours	Best endeavours	Best endeavours	Partial
Source code protection	Binding	Binding	Binding	Not present
Cybersecurity cooperation	Binding	Binding	Binding	Not present
Internet access principles	Not present	Best endeavours	Not present	Not present

Table 4.9.2 Digital trade disciplines across Peru's key agreements

C. Domestic Law - IIA Interaction

An analysis of Peru's domestic digital policy and its treaty practice suggests that its domestic regulatory activities are largely in line with its international obligations. At the domestic level, the overall focus of Peru's digital policy has been on increasing digitalization, improving data protection and cybersecurity, and developing the digital economy. Peru's treaty practice focuses on eliminating trade barriers of digital products and services and promoting international cooperation on digital issues. As such, they are compatible. For example, the Personal Data Protection Law in Peru allows for the cross-border transfer of personal data as long as there are adequate safeguards, which is consistent with Peru's international obligations on free data flows.

The expansion of digital infrastructure and the promotion of digital innovation are domestic priorities that are also reflected in the cooperation provisions included in many of Peru's FTAs, particularly in the digital trade chapters which promote the frameworks of electronic commerce, consumer protection, and digital technology cooperation. These obligations are in line with Peru's policy that aims to integrate digital technologies into the national development agenda.

Peru's digital trade treaty practice has been characterized by a concern to ensure that its domestic digital trade development policies remain consistent with WTO obligations. By agreeing to digital trade agreements that balance the promotion of digital trade with the protection of domestic regulatory authority, Peru seeks to achieve the development of its digital economy, attract investment, and enhance its competitiveness in the international digital economy.

It is worth recalling that Peru has adopted a Model BIT 2018, which has been already invoked during consultations held in 2020. The Model BIT, which would apply to foreign investors in the digital economy, includes provisions on investments in this sector. As is the case with any investment, foreign-owned digital economy enterprises operating in Peru would benefit from the guarantees and protections contained in Article 4 on Transfers. In turn, foreign-owned digital economy enterprises operating abroad would expect to enjoy fair and equitable treatment, most-favoured-nation treatment, and national treatment (Articles 2 and 3, Model BIT). Additionally, these investors would benefit from the market-access commitments contained in Peru's FTAs, particularly those that establish rules for the digital economy. A potentially contentious interaction is the room available to Peru to establish domestic measures and exceptions regarding data and

cross-border data flows. In the event of a foreign digital economy investor alleging an impairment of their investment in Peru by such a measure, the corresponding BIT standards would come into play. This is an evolving area of international investment law, and Peru's policymakers should pay close attention to its developments.

There are a few areas where domestic law may not be compatible with treaty obligations. First, the country's Personal Data Protection Law of 2011 predates much of Peru's digital trade commitments, and does not address other international systems for protecting personal information, such as APEC's Cross-Border Privacy Rules to which several CPTPP countries are parties. The HK-Peru FTA should encourage parties to develop ways to foster compatibility between their data protection regimes, and accordingly, encourage Peru to accede to the CBPRs system. Second, Peru currently does not have a law regulating cybersecurity, whereas PECERT exists only in administrative form without enabling legislation and may struggle to meet its obligations under the CPTPP and HK-Peru FTA with respect to matters of cybersecurity cooperation. Finally, the Digital Government Framework Law could be used more effectively to fulfill paperless trading commitments under FTAs by making the government's digitalization agenda more relevant to trade facilitation goals, rather than merely focusing on interoperability among different government agencies and entities.

Domestic Area	**Relevant Instrument(s)**	**Current Alignment**	**Notes / Gaps**
Cross-border data transfers	Law No. 29733	Generally aligned	Safeguard-based framework consistent with FTA data flow provisions
Data protection framework modernity	Law No. 29733 (2011)	Partial: law is dated	Does not engage APEC CBPR or comparable modern standards
Cybersecurity capacity	PECERT (administrative)	Partial	No dedicated cybersecurity law; PECERT mandate may be limited without legislation
Digital public services	Digital Gov. Framework Law	Aligned	Foundation for paperless trading commitments
Digital investment protections	2020 Model BIT	Generally compatible	Potential tension between data regulation and BIT transfer rights
E-commerce consumer protection	Consumer Protection Code	Generally aligned	FTA obligations require adoption of anti-fraud/deceptive practices measures

Electronic authentication	Not specifically legislated	Uncertain	FTAs require legal validity of e-signatures (Gap if not in domestic law)

Table 4.9.3 Domestic law alignment with digital trade obligations

4.10. Rwanda

Rwanda has an ambitious domestic digital governance framework which is in tension with its expanding international commitments. Domestically, Rwanda has one of the most sustained digital transformation agendas on the African continent, positioning information and communications technology as a central driver of its national development strategy. Its treaty practice is shaped primarily by continental frameworks, as well as membership in regional economic communities. Rwanda's approach reflects a 'regulate first, negotiate second' strategy: building strong domestic regulatory capacity before engaging in treaty commitments, then adapting domestic law iteratively to accommodate international obligations. However, one critical tension remains urgent, particularly between its strict data localization mandate and the AfCFTA's prohibition on mandatory local computing facilities.

A. Domestic Digital Policies

Rwanda has one of the most ambitious digital transformation agendas on the African continent, positioning information and communications technology as a central driver of its development strategy. Rwanda's long-term development framework, Vision 2050, identifies technology and innovation as a core pillar of the country's aspiration to transition from a low-income, agrarian economy to an upper middle-income country by 2035 and a high-income by 2050.[105]

The institutional digital policy architecture is led by the Ministry of ICT and Innovation, which is responsible for policy design, direction, and coordination of the ICT sector. The operational implementation of e-government initiatives is entrusted to the Rwanda Information Society Authority, while cybersecurity and data protection enforcement fall under the National Cyber

[105] Government of Rwanda, Vision 2050 (Government of Rwanda 2020).

Security Authority (NCSA), established by Law No 26/2017.[106] This institutional arrangement distinguishes Rwanda's digital governance model from that of many developing countries.

A succession of strategic plans has guided Rwanda's digital development. The National Information and Communications Infrastructure (NICI) Plans, spanning from 2000 to 2015 in four phases, laid the groundwork for digital infrastructure, institutional capacity, and e-government services. These were succeeded by the Smart Rwanda Master Plan (SRMP, 2015–2020), which set the goal of transforming Rwanda into a knowledge-based economy through three pillars: SMART Government, SMART Economy, and SMART Citizen.[107] The SRMP achieved near-universal 4G population coverage (achieved at 98 percent), expanded broadband infrastructure to over 21,800 kilometers of fiber optic network, digitized 89 government services, and established enabling policy, regulatory, and institutional frameworks.[108]

The current framework is set out in the ICT Sector Strategic Plan 2024-2029 (ICT SSP), which prioritizes three areas: accelerating digital transformation; promoting digital inclusion through accessible and secure ICT infrastructure; and enhancing digital service delivery through improved governance and innovation.[109]

In the area of data protection, Rwanda's primary legislative instrument is Law No 058/2021 of 13/10/2021 on the Protection of Personal Data and Privacy (Data Protection Law), which entered into force on 15 October 2021.[110] This law represents Rwanda's first comprehensive data protection legislation. It establishes a framework for covering lawful bases for processing, data subject rights (including access, rectification, erasure, restriction, portability, and objection), mandatory designation of data protection officers for certain categories of controllers and processors, data breach notification requirements, and a detailed enforcement regime with

[106] Law No 26/2017 of 31/05/2017 Establishing the National Cyber Security Authority and Determining its Mission, Organisation and Functioning (Government of Rwanda).
[107] Smart Rwanda Master Plan (SRMP) 2015–2020, approved by Cabinet 3 November 2015.
[108] Ministry of ICT and Innovation, ICT Sector Strategic Plan 2018–2024 (Government of Rwanda 2018).
[109] Ministry of ICT and Innocavation, ICT Sectror Strategic Plan 2024–2029 (Government of Rwanda 2024)
[110] Law No 058/2021 of 13/10/2021 relating to the Protection of Personal Data and Privacy (Data Protection Law, Government of Rwanda 2021)

administrative, civil, and criminal penalties. Notably, the Data Protection Law applies extraterritorially. [111]

Regarding cross-border data transfers, the Data Protection Law permits transfers outside Rwanda subject to authorization from the supervisory authority, data subject consent, contractual necessity, public interest, or certain other specified grounds.[112] Rwanda's international commitments in this area are reinforced by its ratification of the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) in November 2019, by Presidential Order No 104/01 of 18/09/2019.[113] The Malabo Convention, which entered into force on 8 June 2023, establishes continent-wide standards for electronic commerce, data protection, and cybersecurity, and Rwanda was among the first fifteen states to ratify it.

Rwanda's cybersecurity framework is anchored by the NCSA, which coordinates national efforts to secure cyberspace, operates the Rwanda Computer Security Incident Response Team (Rw-CSIRT), and oversees compliance with data protection and cybersecurity legislation.[114]

Additional elements of the digital governance landscape include the National Data Revolution Policy (2017), which established principles for data-driven policymaking,[115] and Rwanda's pioneering e-waste legislation (2016), which made the country one of the first globally with dedicated national legislation on electronic waste management.

Overall, Rwanda's domestic digital policy framework is characterised by a high degree of strategic coherence, institutional maturity, and progressive regulatory ambition. The country's iterative approach to strategy development, its commitment to continental frameworks such as the Malabo Convention, has positioned it as a leading digital governance actor in sub-Saharan Africa.

---

[111] Hogan Lovells, 'Key Features of the New Rwandan Data Protection Law' (2021) <https://www.hoganlovells.com/en/publications/key-features-of-the-new-rwandan-data-protection-law> accessed 19 March 2026characterizedpercentave.o and its commitment to continental frameworks such as the Malabo Convention have

[112] Data Protection Law, art 48(1)–(3).

[113] African Union Convention on Cyber Security and Personal Data Protection (adopted 27 June 2014, entered into force 8 June 2023) (Malabo Convention). Rwanda ratified by Presidential Order No 104/01 of 18/09/2019.

[114] Digital Watch Observatory, 'Rwanda's National Cyber Security Policy' (11 January 2024) <https://dig.watch/resource/rwandas-national-cyber-security-policy> accessed 16 March 2026.

[115] National Data Revolution Policy (Government of Rwanda 2017).

Challenges remain, however, particularly in digital literacy (estimated at only 10 per cent), smartphone penetration, and the capacity of SMEs to engage with the digital economy.[116]

Year	Instrument	Type
2000	ICT-2020 Policy / NICI I	Domestic policy
2006–2010	NICI II (National fibre-optic backbone)	Domestic policy
2010	Law No 18/2010 on Electronic Messages, Signatures and Transactions	Domestic law
2015	Smart Rwanda Master Plan (SRMP) 2015–2020	Domestic policy
2017	National Data Revolution Policy	Domestic policy
2017	Law No 26/2017 establishing NCSA	Domestic law
2018	AfCFTA Agreement signed (Kigali)	Treaty
2018	Rwanda deposits AfCFTA ratification (3rd country)	Treaty
2018	Singapore-Rwanda BIT signed	Treaty
2019	Malabo Convention ratified (Presidential Order 104/01)	Treaty
2021	Data Protection Law No 058/2021 enters into force	Domestic law
2023	AfCFTA Investment Protocol adopted	Treaty
2024	AfCFTA Digital Trade Protocol adopted	Treaty
2024	ICT SSP 2024–2029	Domestic policy

Table 4.10.1 - Timeline of Key Domestic and Treaty Instruments

B. *Treaty Practice in the Digital Sphere*

Rwanda's treaty practice in the digital sphere is shaped by its engagement at multiple levels of international economic governance: its foundational role in the African Continental Free Trade Area ('AfCFTA'), its membership in regional economic communities including the East African Community ('EAC') and the Common Market for Eastern and Southern Africa ('COMESA'), and its network of BITs. The treaties that will be discussed in this section are the following:

- The Protocol to the Agreement Establishing the African Continental Free Trade Area on Digital Trade (DTP);

- The Protocol to the Agreement Establishing the African Continental Free Trade Area on Investment (AfCFTA Investment Protocol);

[116] ICT SSP 2024–2029, Ch 2.2.

• The East African Community digital trade frameworks; and

• Rwanda's BITs.

Rwanda hosted the AfCFTA Agreement ceremony and was among the first countries to ratify it. The agreement entered into force on 30 May 2019.[117] The most significant development for Rwanda's digital trade treaty practice is the adoption of the DTP.[118] The DTP addresses market access and the treatment of digital products; the facilitation of digital trade (including electronic authentication, paperless trading, electronic contracts, digital identities, and digital payments); data governance (encompassing cross-border data transfers, protection of personal data, and provisions on source code); consumer trust and online consumer protection; cybersecurity; emerging and advanced technologies; and digital inclusion.[119]

The DTP's general objective is to "support the attainment of the objectives of the AfCFTA... by establishing harmonised rules and common principles and standards that enable and support digital trade for sustainable and inclusive socio-economic development and the digital transformation of the continent."[120] Article 4 preserves each State Party's "right to regulate within its territory to safeguard public welfare, promote sustainable development, protect essential security interests and pursue legitimate public policy objectives."

On cross-border data flows, Article 20(1) mandates that "State Parties shall, subject to an Annex on Cross-Border Data Transfers, allow the cross-border transfer of data, including personal data, by electronic means, provided the activity is for the conduct of digital trade by a person of a State Party." However, Article 20(2) permits derogation where a State Party adopts measures "to achieve a legitimate public policy objective or protect essential security interests, provided that the measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable

[117] Agreement Establishing the African Continental Free Trade Area (signed 21 March 2018, entered into force 30 May 2019) (AfCFTA Agreement).
[118] Protocol to the Agreement Establishing the African Continental Free Trade Area on Digital Trade, adopted by the AU Assembly (17–18 February 2024, Addis Ababa) (AfCFTA Digital Trade Protocol).
[119] Kholofelo Kugler, 'The AfCFTA Digital Protocol' (IISD, October 2024) <https://www.iisd.org/articles/policy-analysis/afcfta-digital-protocol> accessed 16 March 2026.
[120] AfCFTA Digital Trade Protocol, art 2(1).

discrimination, or a disguised restriction on digital trade, and do not impose restrictions on transfers of data greater than are necessary to achieve the objective."

On data localization, Article 22(1) prohibits requiring "a person of another State Party to use or locate computing facilities in their territories as a condition for conducting digital trade in that territory," subject to the same necessity-based exceptions. Crucially, Article 22(3) contains a negotiated compromise: States shall "encourage and support the establishment and use of computing facilities within State Parties to promote the development of local digital infrastructure and access."

Source code protection under Article 24(1) prevents States from requiring "the transfer of, or access to, a source code of software owned by a person of another State Party, or an algorithm expressed in that source code, as a condition for the import, distribution, sale or use of that software." The DTP also carves out exceptions for regulatory bodies and judicial authorities requiring access "for a specific investigation, inspection, examination, audit, enforcement action, or judicial proceeding," subject to safeguards against unauthorized disclosure.[121] Consumer protection provisions in Article 27 require States to adopt laws prohibiting "misleading, fraudulent, and deceptive commercial activities or practices that cause harm or have the potential to cause harm to consumers engaged in digital trade."

Full implementation of the AfCFTA Digital Trade Protocol is estimated to increase digital trade integration scores by an average of 313 percent for participating nations, with particularly significant gains in policy areas where virtually no international commitments previously existed, such as trust and e-commerce, cross-border data flows, and wider digital economy governance.[122] The Protocol has been described as comparable in ambition and scope to leading digital trade agreements globally, though adapted to the specific needs and capacities of African economies, 33 of which are classified as least developed countries.[123]

[121] AfCFTA Digital Trade Protocol, art 24(1)–(3).
[122] OECD, 'The OECD's New Index of Digital Trade Integration Shows Strong Gains from the AfCFTA's Digital Trade Protocol' (tralac, 2025) <https://www.tralac.org/blog/article/16912> accessed 16 March 2026.
[123] Franziska Sucker, 'The AfCFTA Digital Trade Protocol' (SSRN, August 2025) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5386851> accessed 16 March 2026.

Alongside the DTP, the AfCFTA Protocol on Investment, adopted in February 2023, establishes continental investment governance standards that are relevant to the digital economy.[124] The Protocol employs an enterprise-based investment definition rather than the broad asset-based formulations typical of older BITs. "Investment" requires "commitment of capital or other resources, the expectation of gain or profit, a certain duration, assumption of risk, and a significant contribution to the Host State's sustainable development."[125] Most significantly, Article 17 replaces traditional fair and equitable treatment standard with an "administrative and judicial treatment" provision, ensuring investors are not subject to "a fundamental denial of justice in criminal, civil and administrative adjudicative proceedings, an evident denial of due process, a manifest arbitrariness," or "discrimination based on gender, race or religious beliefs." Article 17(2) states this "shall not be interpreted as equivalent to fair and equitable treatment."

Article 24's right-to-regulate provision affirms that "each State Party has the right to regulate, including to take measures to ensure that investment in its territory is consistent with the goals and principles of sustainable development." Critically, Article 24(3) provides that exercise of this right "cannot give rise to any claim by an investor for compensation." The Protocol's investor obligations provisions, covering business ethics, environmental protection, anti-corruption, and corporate governance, create reciprocal responsibilities absent from Rwanda's existing BITs.[126] Article 49 mandates termination of existing intra-African BITs within five years. The DTP cross-references the Investment Protocol directly: Article 36(c) requires States to "promote and facilitate investments in the ICT sector and promote the cross-border transfer of such technology, skills, and know-how in accordance with the Protocol on Investment."

At the regional level, Rwanda's membership in the EAC and COMESA provides additional layers of economic integration with investment-relevant provisions. The EAC became the first region in Africa to adopt a harmonised framework for cyberlaws when its Framework for Cyberlaws was endorsed by the Council of Ministers.[127] The EAC E-Commerce Strategy, adopted on 12 July

[124] Protocol to the Agreement Establishing the African Continental Free Trade Area on Investment, adopted by the Assembly of the African Union (February 2023) (AfCFTA Investment Protocol).
[125] AfCFTA Investment Protocol, art 1.
[126] AfCFTA Investment Protocol, arts 31–40.
[127] UNCTAD, 'Harmonizing Cyberlaws and Regulations: The Experience of the East African Community' (2012) <https://unctad.org/publication/harmonizing-cyberlaws-and-regulations-experience-east-african-community> accessed 16 March 2026.

2022, aims to establish an "EAC Single Digital Market" with seamless cross-border transactions.[128] COMESA contributes model legislation: the Model Law on Electronic Transactions (2010) and the Cyber Crime Model Bill (October 2011) provide templates for national transposition.[129]

Rwanda's BIT practice includes active agreements with Germany (1969), the Belgium-Luxembourg Economic Union (1985), the Republic of Korea (2013), the UAE (2017), and Singapore (2018). However, like the majority of existing BITs globally, Rwanda's bilateral treaties follow traditional investment treaty structures with standard protections relating to expropriation, fair and equitable treatment, national treatment, most-favored-nation treatment, and investor-state dispute settlement, without explicit provisions addressing the digital economy, data governance, or cross-border data flows. The UAE-Rwanda BIT (2017) is the most relevant as it contains a right-to-regulate clause in Article 9 covering public health, security, environment, and labor, though notably not data protection or digital regulation specifically.

Policy Domain	**Domestic Framework**	**Treaty Provisions**	**Alignment**
Data protection	Law No 058/2021: comprehensive framework; breach notification within 48 hours; extraterritorial application	AfCFTA Digital Trade Protocol art 21: requires adoption of data protection framework; Malabo Convention ratified	Aligned
Data localization	Strict domestic storage requirement; NCSA authorization for offshore storage	AfCFTA art 22(1): prohibits mandatory localization for digital trade	**Tension**
Cross-border data flows	Permitted with NCSA authorization or adequate safeguards	AfCFTA art 20(1): requires allowing transfers for digital trade conduct	Partial
E-transactions	Law No 18/2010: legal recognition of electronic signatures and contracts	AfCFTA art 12: electronic contracts legally valid; EAC Framework	Aligned

[128] East African Community, 'EAC E-Commerce Strategy' (adopted 12 July 2022).

[129] Digital Watch Observatory, 'COMESA Model Law on Electronic Transactions' (2010) <https://dig.watch/resource/comesa-model-law-electronic-transactions> accessed 16 March 2026.

Cybersecurity	NCSA (Law 26/2017); Rw-CSIRT; critical infrastructure protection	AfCFTA art 25: cooperation provisions; EAC Cyberlaw Framework	Aligned
Consumer protection	Data Protection Law consumer provisions; Competition Authority	AfCFTA art 27: prohibition on misleading practices; redress mechanisms	Aligned
Source code	No explicit domestic regulation	AfCFTA art 24: prohibits mandatory transfer requirements	Not engaged
Digital infrastructure	SRMP; 98% 4G coverage; 21,800 km fibre; ICT SSP 2024-2029	AfCFTA art 22(3): encourages local facility establishment; art 36	Aligned
Investment protection	No digital-specific investment law	BITs: traditional protections without digital provisions; AfCFTA Investment Protocol: sustainable development focus	Gap (closing)

Table 4.10.2 - Domestic Digital Policy vs Treaty Provisions: Comparative Overview

C. *Domestic law - IIA Interaction*

An analysis of Rwanda's shows a clear, development-focused, and cohesive approach to digital governance marked by a strategic sequence: first, strengthen domestic institutions and regulatory frameworks; then, participate in treaty-making, leveraging that institutional strength. The interaction between domestic law and international investment agreements operates in both directions, with Rwanda shaping and being shaped by its international commitments.

The chronological order of Rwanda's digital governance instruments demonstrates that domestic policy development preceded and informed treaty engagement. By the time Rwanda hosted the AfCFTA signing ceremony, the country had already completed three phases of NICI planning and implemented the Smart Rwanda Master Plan. The Data Protection Law entered into force more than two years before the DTP was adopted in 2024. This sequence of steps helped Rwanda join continental discussions with a solid regulatory framework already in place.

Looking at the treaty to national policy influence, one particular challenge emerges. The DTP will require adjustments to Rwanda's domestic regulatory framework within the five-year implementation period. The most significant tension lies in data localization. Rwanda's Data Protection Law requires personal data to be stored within Rwanda unless entities obtain NCSA-

issued certificates for offshore storage.[130] The DTP's Article 22(1), by contrast, prohibits requiring "a person of another State Party to use or locate computing facilities in their territories as a condition for conducting digital trade."

The WTO-World Bank Digital Trade for Africa report (2025) explicitly notes that Rwanda's "current regulations lack measures that limit data localization requirements", meaning Rwanda's localization rules exceed what the AfCFTA will permit.[131]

4.11. Saudi Arabia

Saudi Arabia has domestically driven digital governance that significantly outpaces its treaty commitments. Under Vision 2030, the Kingdom has built a comprehensive regulatory architecture. Notably, the Kingdom has not imposed blanket data localization requirements. At the treaty level, Saudi Arabia's digital commitments are embedded in multilateral (JSI), regional (GCC), and bilateral (TIFA) frameworks rather than in standalone digital economy agreements. Its BIT network follows traditional investment protection models with no explicit digital provisions. The direction of influence is predominantly domestic to international: Vision 2030's diversification imperatives have driven regulatory innovation, while treaty obligations have provided baseline market access commitments without shaping the domestic agenda.

A. Domestic Digital Policies

Saudi Arabia (KSA) has positioned digital transformation as a central pillar of its national development strategy. Under the Vision 2030 development framework, launched in April 2016, KSA has embarked on a comprehensive programme of economic diversification aimed at reducing dependence on hydrocarbon revenues and building a knowledge-based economy.[132] Digital development is embedded across multiple institutional and regulatory instruments and is coordinated through a dedicated network of government agencies.

[130] Data Protection Law, art 48; National Bank of Rwanda, Regulation No 02/2018.
[131] WTO and World Bank, 'Digital Trade for Africa (DTA): Rwanda Report' (2025) <https://www.wto.org/english/tratop_e/serv_e/rwanda-report-digital-trade-for-africa-initiative_e.pdf> accessed 16 March 2026.
[132] Saudi Vision 2030, 'Overview' <https://www.vision2030.gov.sa/en/overview> accessed 19 March 2026.

Nationally, the principal strategic instrument is the National Transformation Programme ('NTP'), launched in 2016 as one of the first Vision 2030 realization programmes. The NTP identifies digital transformation as a cross-cutting theme, emphasising the digitalization of government services, the development of primary and digital infrastructure, and the enablement of private-sector participation in the digital economy.[133] A complementary Digital Government Strategy, first issued in 2023 and revised for the period 2025–2030, sets out KSA's ambition to position itself among the top three countries globally in digital government maturity by 2030.[134]

Institutional responsibilities for the digital economy are distributed across several specialised agencies. The Digital Government Authority ('DGA'), established to coordinate and regulate digital government activities, oversees the adoption of emerging technologies, interoperability standards, and digital-by-design principles across government entities.[135] KSA's Data and AI Authority ('SDAIA'), created by Royal Decree in August 2019, serves as its central authority for data governance and AI.[136] SDAIA launched the National Strategy for Data and AI ('NSDAI') in October 2020, setting targets that include ranking among the top fifteen countries in AI, attracting SAR 75 billion (approximately USD 20 billion) in data and AI investment, and training over 20,000 specialists by 2030.[137]

In the area of data protection, KSA's primary legislative instrument is the Personal Data Protection Law ('PDPL'), enacted by Royal Decree No. M/19 on 16 September 2021 and subsequently amended by Royal Decree No. M/148 on 27 March 2023.[138] The PDPL is KSA's first comprehensive data protection legislation and establishes a unified framework governing the collection, processing, storage, and transfer of personal data across both public and private sectors. The law grants data subjects rights of access, rectification, and erasure, and imposes obligations

[133] Saudi Vision 2030, 'National Transformation Program' <https://www.vision2030.gov.sa/v2030/vrps/ntp/> accessed 19 March 2026.
[134] Digital Government Authority (DGA), 'Digital Government Strategy' <https://my.gov.sa/en/content/digital-strategy> accessed 19 March 2026.
[135] DGA, 'Digital Transformation' <https://dga.gov.sa/en/digital-transformation> accessed 19 March 2026.
[136] Saudi Data and Artificial Intelligence Authority (SDAIA), 'About SDAIA' <https://sdaia.gov.sa/en/default.aspx> accessed 19 March 2026.
[137] 'National Strategy for Data and AI (NSDAI)' (Saudipedia) <https://saudipedia.com/en/article/2878/economy-and-business/data-and-ai/national-strategy-for-data-and-ai-nsdai> accessed 19 March 2026.
[138] Personal Data Protection Law (PDPL), issued by Royal Decree No M/19 (16 September 2021), amended by Royal Decree No M/148 (27 March 2023).

on data controllers, including consent requirements, breach notification duties, and data protection officer appointment mandates. Enforcement is vested in SDAIA as the competent supervisory authority.[139] Importantly, the 2023 amendments aligned the PDPL more closely with international norms. The updated version introduced a legitimate interest basis for processing and liberalising the cross-border data transfer regime. It permits transfers where the recipient jurisdiction provides adequate protection or where transfers are necessary for the performance of contractual obligations, subject to conditions to be further specified in implementing regulations.[140] Separate Regulations on Personal Data Transfer outside KSA have also been issued, establishing evaluation criteria for adequacy assessments.[141]

Cybersecurity governance is institutionalized within the National Cybersecurity Authority, established by Royal Decree in October 2017.[142] Its responsibilities include drafting and supervising the implementation of the national cybersecurity strategy, setting cybersecurity policies, governance rules, frameworks, and standards, and classifying critical national infrastructure. The NCA has issued a suite of mandatory cybersecurity controls, including the Essential Cybersecurity Controls, Cloud Cybersecurity Controls, Critical Systems Cybersecurity Controls, and the National Cryptographic Standards (NCS-1:2020).[143] These frameworks are complemented by the Anti-Cyber Crime Law, first enacted in 2007 and revised in 2015, which criminalises unauthorised access, data interference, fraud, and electronic forgery.[144]

The E-Commerce Law was issued by Royal Decree No. M/126 on 9 July 2019, accompanied by Implementing Regulations adopted on 31 January 2020.[145] The law regulates electronic

[139] Ibid, arts 4-12 (data subject rights), arts 14-18 (controller obligations). See also ICLG, 'Data Protection Laws and Regulations: Saudi Arabia' (2025) <https://iclg.com/practice-areas/data-protection-laws-and-regulations/saudi-arabia> accessed 19 March 2026.

[140] 'Saudi Arabia's Updated Personal Data Protection Law' (Lexology, 3 May 2023) <https://www.lexology.com/library/detail.aspx?g=505a26e5-7c71-44a7-a355-a38195ee80db> accessed 19 March 2026.

[141] Regulation on Personal Data Transfer outside the Kingdom, issued pursuant to the PDPL. See DLA Piper, 'Data Protection Laws of the World: Saudi Arabia' <https://www.dlapiperdataprotection.com/?c=SA> accessed 19 March 2026.

[142] National Cybersecurity Authority (NCA), 'About NCA' <https://nca.gov.sa/en/vision-and-mission/> accessed 19 March 2026.

[143] NCA, 'Cybersecurity in the Kingdom' (National Platform) <https://my.gov.sa/en/content/cybersecurity> accessed 19 March 2026.

[144] Anti-Cyber Crime Law, Royal Decree No M/17 (26 March 2007), revised 2015.

[145] 'E-commerce Law in Saudi Arabia' (Saudipedia) <https://saudipedia.com/en/e-commerce-law-in-saudi-arabia> accessed 19 March 2026.

commercial transactions, imposes disclosure and consumer protection obligations on e-commerce service providers, addresses the protection of consumer personal data in the context of online transactions, and establishes penalties for violations. The earlier Electronic Transactions Law provides legal recognition to electronic contracts, signatures, and records.[146]

Overall, KSA's domestic digital policy framework has a high degree of institutional ambition, substantial public investment, and a rapidly maturing regulatory architecture. In under a decade, KSA has built a unified governance model spanning cybersecurity, data privacy, and AI. However, challenges persist, particularly in ensuring consistent compliance across sectors, bridging the digital divide, and harmonising overlapping regulatory mandates.

Year	Instrument	Type
1996–2024	Network of bilateral investment treaties (BITs)	Treaty (bilateral)
2001	GCC Revised Economic Agreement	Treaty (regional)
2003	Saudi Arabia–US TIFA	Treaty (bilateral)
2005	WTO Accession	Treaty (multilateral)
2007	Anti-Cyber Crime Law	Domestic legislation
2016	Vision 2030 and National Transformation Programme	Domestic strategy
2017	National Cybersecurity Authority established	Domestic institution
2019	E-Commerce Law (Royal Decree M/126)	Domestic legislation
2019	Saudi Data and AI Authority (SDAIA) established	Domestic institution
2020	National Strategy for Data and AI (NSDAI)	Domestic strategy
2021	Personal Data Protection Law (PDPL)	Domestic legislation
2023	PDPL Amendments (Royal Decree M/148)	Domestic legislation
2023	Digital Government Strategy (1st edition)	Domestic strategy
2024	WTO Agreement on Electronic Commerce (stabilised text)	Treaty (plurilateral)
2025	Digital Government Strategy (2025–2030 revision)	Domestic strategy

Table 4.11.1 - Timeline of Key Domestic and Treaty Instruments

B. Treaty Practice in the Digital Sphere

Saudi Arabia's treaty practice in the digital sphere is shaped by three principal vectors:

[146] Electronic Transactions Law, Cabinet Decision No 80 (19 March 2007).

(1) its membership in the Gulf Cooperation Council ('GCC');

(2) its participation in the WTO, including the JSI on Electronic Commerce; and

(3) its extensive network of BITs and trade and investment framework agreements.

At the regional level, the GCC Economic Agreement, originally adopted in 1981 and substantially revised in 2001, provides the overarching framework for economic integration. The revised agreement calls on member states to facilitate commercial exchange through electronic communications and to unify legislation related to e-commerce.[147] However, the GCC framework does not contain a dedicated digital trade chapter with specific disciplines on cross-border data flows, data localization, or source code protection. The GCC is currently negotiating FTAs with external partners, including the ongoing GCC–UK FTA negotiations initiated in June 2022, which are expected to cover digital services.[148]

At the multilateral level, KSA became a member of the WTO in 2005. Its WTO commitments govern market access in services, including telecommunications, and provide the baseline rules for electronic commerce under GATS and the WTO Work Programme on Electronic Commerce. Significantly, KSA is an active participant in the JSI.[149] In 2024, the JSI participants agreed on a text for the Agreement on Electronic Commerce, establishing baseline disciplines on electronic signatures and authentication, paperless trading, electronic contracts, electronic invoicing, consumer protection online, and cross-border data flows.[150]

KSA also signed a Trade and Investment Framework Agreement ('TIFA') with the United States in July 2003, which provides a structured dialogue platform on trade liberalization, investment

[147] The Economic Agreement between the Countries of the Gulf Cooperation Council (revised, 21 December 2001) ch 7, art 25.
[148] Simeon Kerr, 'UK seeks Gulf trade boost as talks start to secure deal' *Financial Times* (21 June 2022) <https://www.ft.com/content/aa6b3790-f964-4cfe-9ceb-b326530c98f1> accessed 19 March 2026.
[149] WTO, 'Joint Statement Initiative on E-commerce' <https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm> accessed 19 March 2026. Saudi Arabia is listed among the 91 participating members.
[150] 'Saudi Arabia Participates in Recent WTO E-commerce Agreement' (Sovereign Group, 1 October 2024) <https://www.sovereigngroup.com/news/saudi-arabia-participates-in-recent-wto-ecommerce-agreement/> accessed 19 March 2026.

protection, intellectual property, and customs transparency. However, it does not contain specific digital trade disciplines.[151]

KSA's BIT practice is structurally traditional. KSA has numerous BITs, including agreements with France (2002), India (2006), Spain (2006), Jordan (2017), and Egypt (2024), among others. These BITs follow conventional investment protection models, providing for fair and equitable treatment, full protection and security, expropriation standards, and investor-state dispute settlement. However, they do not typically include explicit references to the digital economy, digital trade, data governance, cross-border data flows, or data localization requirements.

Unlike some countries that have begun negotiating standalone DEAs, KSA has not yet concluded a dedicated digital trade agreement. Its digital trade commitments are instead embedded within the multilateral WTO, regional GCC, and bilateral TIFA frameworks described above. This approach mirrors the pattern observed in many Gulf states, where digital trade governance has developed primarily through domestic regulation rather than through treaty-based disciplines.

Policy Domain	Domestic Framework	Treaty Provisions	Alignment
Data protection	PDPL: comprehensive rights-based framework; SDAIA as supervisory authority.	WTO JSI: consumer protection and personal information provisions. GCC: no specific data protection disciplines. BITs/TIFA: silent.	Partial
Data localization	No blanket data localization mandate under PDPL; cross-border transfers permitted subject to adequacy safeguards.	WTO JSI: disciplines on cross-border data flows. GCC: no specific provisions. BITs/TIFA: silent.	Aligned
Cybersecurity	NCA: ECC, CCC, CSCC, NCS standards; Anti-Cyber Crime Law.	WTO JSI: no binding cybersecurity disciplines. GCC: no cybersecurity framework. BITs/TIFA: silent.	Gap
E-commerce	E-Commerce Law and Implementing Regulations: consumer protection, disclosure, electronic advertising.	WTO JSI: electronic signatures, paperless trading, e-contracts, consumer protection. GCC: calls for e-commerce legislation unification.	Aligned
E-signatures	Electronic Transactions Law: legal recognition of e-signatures and e-contracts.	WTO JSI: e-signatures and authentication disciplines. GCC: interoperability commitment. BITs: silent.	Aligned
Source code	No domestic legislation on source code disclosure.	WTO JSI: not addressed in stabilised text. GCC/BITs/TIFA: not addressed.	Absent

[151] 'Saudi Arabia – Trade Agreements' (International Trade Administration) <https://www.trade.gov/country-commercial-guides/saudi-arabia-trade-agreements> accessed 19 March 2026.

Cross-border data flows	PDPL permits transfers subject to adequacy assessment; Transfer Regulations issued by SDAIA.	WTO JSI: cross-border data flow disciplines (pending integration). GCC: no provisions. BITs/TIFA: silent.	Partial
AI governance	NSDAI; SDAIA AI Ethics Principles; AI Adoption Framework; dedicated AI law under development.	No treaty-level AI governance provisions applicable to Saudi Arabia.	Gap
Digital infrastructure	NTP and Digital Government Strategy 2025-2030: smart cities, 5G, data centres, cloud computing.	GCC: infrastructure integration commitments. WTO: telecom commitments. BITs: broad asset definitions.	Partial
Fintech regulation	SAMA Payment Service Provider Regulations; central bank digital oversight.	WTO JSI: electronic payments provisions. GCC: no specific fintech disciplines. BITs/TIFA: silent.	Partial

Table 4.11.2 - Domestic Digital Policy vs Treaty Provisions: Comparative Overview

C. Domestic Law - IIA Interaction

As the above table shows, the relationship between KSA's domestic digital policies and its treaty commitments is characterised by a significant asymmetry. KSA's domestic regulatory framework is noticeably more developed than its treaty-based obligations. Three main trends stand out.

First, KSA demonstrates significant regulatory proactivity by aligning its national laws with emerging global standards well before formal treaty commitments. A primary example of this is the introduction of PDPL, which closely correlates to core principles derived from the General Data Protection Regulation, such as data subject rights, purpose limitation, and content-based processing; contrary to disciplines developed under the JSI. Similarly, the absence of a blanket data localization requirement under the PDPL means that KSA would not face the kind of compliance tension that countries with strict localization mandates may encounter upon integration of WTO e-commerce rules.

Second, the direction of influence in KSA's digital governance is predominantly domestic-to-international. KSA's domestic digital policy framework has developed largely autonomously, driven by Vision 2030's economic diversification imperatives rather than by external treaty obligations. The NCA's cybersecurity controls, SDAIA's data governance framework, and the NSDAI's AI strategy all reflect a nationally driven agenda. Treaty obligations have provided a baseline of market access commitments but have not been the primary driver of regulatory innovation. In this sense, KSA is developing its digital governance model through an autonomous, domestically-led process.

Third, the same gap persists between KSA's rapidly advancing domestic digital governance framework and the limited digital content of its BITs. As KSA's digital economy continues to expand, the absence of digital-specific investment protections in its BIT network represents a notable gap that modernised agreements could address.

In summary, KSA's domestic-treaty interaction in the digital sphere is characterised by a domestically driven, rapidly maturing governance framework that is ahead of the Kingdom's treaty-based digital trade commitments. The primary direction of influence operates from the domestic level to the international level, with the Kingdom developing comprehensive digital policies in pursuit of its development objectives rather than in response to external treaty obligations. As KSA deepens its engagement with multilateral digital trade rule-making and negotiates new trade agreements through the GCC, it will have the opportunity to export elements of its domestic digital governance model into its treaty practice, potentially shaping regional and global digital trade norms.

4.12. Singapore

Singapore presents an advanced case study of both domestic policies and international treaty practice, and how the two are aligned and mutually supportive. Domestically, its digital policies are complex and are supported by primary and secondary legislation and numerous voluntary and industry-led governance guidelines. Its treaty practice includes a new model for DEAs as standalone agreements, as well as incorporating more in-depth provisions on digital economy issues into its FTAs and plurilateral agreements. Singapore has successfully harnessed its international agreements to further its domestic digital agenda and vice versa. Thus, the country has relied on its domestic laws to fulfill its international commitments. This symbiotic bond has further strengthened this model. This is crucial for a balanced development of domestic and international digital governance that ultimately ensures consistency and coherence of rules.

A. Domestic Digital Policy Framework

Singapore's domestic digital policy is highly developed and closely linked to the overall national economic development strategy. The country aspires to be a global digital node and has therefore implemented policies to promote open digital trade, while at the same time imposing necessary regulations to ensure data governance, cybersecurity, the use of AI, and digital infrastructure.

At the national level, digital transformation is carried out through the Smart Nation Initiative launched in 2014. The main objective of this programme is to embed digital technologies in the public administration, economy, and society, with the aim of increasing the global competitiveness of the economy and improving public services. This programme is based on the massive adoption of new digital technologies such as AI, data analytics, or digital identity, among others. Thus, the digital infrastructure becomes fundamental for the country's development, and Singapore intends its digital economy to become a global reference.[152]

Furthermore, the Electronic Transactions Act, introduced in 2010, provides a legal foundation for electronic commerce by giving legal recognition to electronic contracts, records, and signatures. This helps build trust in online transactions, which is crucial for Singapore's plan to grow its digital economy. The Act is also related to international agreements, such as the Singapore-Australia DEA and the UK-Singapore DEA. These agreements have provisions on electronic transactions that are based on the same principles as the Electronic Transactions Act.

Another important mention is the Digital Economy Framework for Action ('DEFA'), launched in 2018. It has four components: developing digital skills in areas of digital trade, innovation, cyber security, and digital skills for workers. The framework is meant to facilitate the adoption of new technologies and link-ups with the global digital economy to help Singapore become a Global Digital Business Centre and Smart Investment Republic.[153]

The Personal Data Protection Act 2012 ('PDPA') was enacted in 2012, with amendments made in 2019. The PDPA requires private organizations to comply with certain privacy provisions when collecting, using, or disclosing personal data. The Act balances two competing interests. The first is the provision of adequate protection to individuals whose personal data is being collected, used, or disclosed by private organizations. The second is the facilitation of data-driven activities and cross-border data flow in Singapore to support innovation.[154]

The Cybersecurity Act 2018 spells out the governance of cybersecurity in Singapore. Under the Act, the critical information infrastructure sectors (which include the finance, energy, transport,

[152] Smart Nation and Digital Government Office, Smart Nation Initiative (Government of Singapore, 2014), https://www.smartnation.gov.sg

[153] Ministry of Trade and Industry (Singapore), Digital Economy Framework for Action (Singapore, 2018).

[154] Parliament of Singapore, Personal Data Protection Act 2012 (No 26 of 2012) (Singapore, 2012, amended 2020).

and healthcare sectors) are regulated. The regulation aims to give the authorities situational awareness of the various cyber threats and to secure the digital infrastructure of the country. This is part and parcel of the overarching agenda of securing the underlying digital systems in the economy to enable the carrying out of transactions securely and efficiently.[155]

The revised national AI strategy, launched in 2019 and revised in 2023, will promote the development and use of AI in key sectors such as financial services, logistics, smart transportation, as well as healthcare, among others.[156] It will also have to address governance, research and development, as well as the take-up of AI.[157] This has promoted the development and use of AI in key sectors such as financial services, smart transportation, healthcare and logistics. This takes the original plan to the next level aiming to make Singapore a world leader in trusted AI, focusing on developing AI capabilities across all industries, setting a global standard for AI governance. Moreover, to support this strategy, Singapore has created the Model AI Governance Framework, first introduced in 2019 and updated in 2024 to include generative AI, which provides practical advice on how to use AI systems responsibly. These guidelines are in line with Singapore's approach to regulation, which emphasizes collaboration and flexibility. By developing voluntary frameworks alongside stricter regulations, Singapore is creating a unique model for AI governance, one that is reflected in its DEAs.

The digital policy environment is also conducive to fintech and digital payments. The Monetary Authority of Singapore (MAS) has launched a range of initiatives, such as regulatory sandboxes and cross-border digital payments, to foster financial innovation while maintaining appropriate oversight. For example, the Payment Services Act (PSA) (2019), together with its regulations, forms the core framework for licensing and regulating payment service providers, with a particular focus on digital payment tokens and cross-border services offered by entities such as foreign digital wallet providers, cryptocurrency exchanges, and other cross-border payment operators; it sets out the applicable regulatory conditions for these providers and stands as a key piece of legislation governing digital payments and related digital asset activities.

[155] Parliament of Singapore, Cybersecurity Act 2018 (No 9 of 2018) (Singapore, 2018).
[156] Smart Nation and Digital Government Office, National Artificial Intelligence Strategy (Government of Singapore, 2019; updated 2023)
[157] Ibid.

The various elements of Singapore's digital economy strategy, which include clear regulatory frameworks, investment in infrastructure, and support for technological innovation, all complement each other.[158]

Year	Instrument	Type
2010	Electronic Transactions Act (ETA)	Domestic law
2012	Personal Data Protection Act (PDPA)	Domestic law
2014	Smart Nation Initiative	National strategy
2018	Digital Economy Framework for Action (DEFA)	National strategy
2018	Cybersecurity Act	Domestic law
2019	Payment Services Act (PSA)	Domestic law
2019	National AI Strategy (NAIS)	National strategy
2020	Singapore–Australia Digital Economy Agreement	Treaty / DEA
2020	Digital Economy Partnership Agreement (DEPA)	Treaty / DEA
2022	Singapore–United Kingdom DEA (UKSDEA)	Treaty / DEA
2023	National AI Strategy 2.0 (NAIS 2.0)	National strategy
2024	Model AI Governance Framework for Generative AI	Voluntary framework

Table 4.12.1 Timeline of Key Domestic and Treaty Instruments

B. Treaty Practice in the Digital Sphere

The Treaties that will be discussed in this section are the following:

(1) DEPA;
(2) the Digital Economy Agreement for the Pacific Alliance (DEAPA);
(3) the Singapore-Australia Digital Economy Agreement (SADEA);
(4) the Singapore-United Kingdom Digital Economy Agreement (UKSDEA);
(5) the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP);
(6) the Regional Comprehensive Economic Partnership (RCEP).

One of the most important recent digital treaty practices of Singapore is the DEPA concluded with Chile and New Zealand in 2020. Described as the first-ever standalone DEA, DEPA takes a new

[158] Monetary Authority of Singapore, FinTech Regulatory Sandbox Guidelines (Singapore, 2016, updated 2022).

approach to digital rule-making and governance through a more flexible and modular structure. As stated in Article 4.3 of the DEPA Agreement, a party shall:

> *"...not prohibit or restrict the cross-border transfer of information by electronic means where this activity is for the conduct of the business of a covered person."*

This provision is in line with recent developments in digital trade agreements, where cross-border data flows are a central part of digital trade. DEPA is concerned with emerging technologies and cooperation in digital governance. According to the 8th module of the Agreement, the cooperation on the governance of AI and the obligations of the parties are to:

> *"..endeavour to promote the adoption of ethical and governance frameworks that support the trusted, safe and responsible use of artificial intelligence technologies."*

The DEAPA is a new type of plurilateral agreement that seeks to promote digital trade and sustainable development. Rather than centering access to markets like traditional commercial, the DEAPA will promote factors that encourage digital innovation, interoperability, and future developments in fields such as AI, cybersecurity, the IoT, and the development of the cloud.

Singapore has been including more substantial provisions on digital trade in its FTAs. An example is the SADEA, established in 2020. It contains many digital provisions such as online payment, digital identity, data flows, and e-invoicing. Notably, the Agreement includes a dedicated provision concerning electronic transactions. Article 8 of the Agreement deals with electronic transactions as follows:

> *"A Party shall not deny the legal validity of a contract solely on the basis that it is concluded by electronic means."*

The UKSDEA also covers areas of digital trade cooperation, including cross-border data flows, cybersecurity, and digital identities. Article 8 of the agreement states 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."*

This rule is consistent with Singapore's approach to data flow liberalization. Singapore is also a member of several RTAs that have digital trade rules. These include the CPTPP, which has an e-

commerce chapter dealing with cross-border data flows, consumer protection, electronic transactions, and paperless trade. Article 14.11 of the CPTPP states 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.*"

The agreement also restricts data localization requirements. Article 14.13 provides that:

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

These provisions are among the most significant digital trade rules included in a modern trade agreement and prohibit governments from imposing data localization requirements. Singapore is also a member of the RCEP, an FTA that includes an electronic commerce chapter that deals with digital trade facilitation, consumer protection, and digital governance. While the RCEP rules are less prescriptive than those contained in the CPTPP, they provide a basis for countries to engage in cooperation and dialogue on e-commerce regulation.[159]

C. Domestic Law - IIA Interaction

An examination of the relationship between Singapore's domestic digital policy measures and its treaty practice shows a high degree of consistency and consonance between the two. Internationally, Singapore has undertaken commitments to promote digital trade, build strong digital economy infrastructure, and avoid using domestic measures that create trade barriers. These commitments are echoed in the country's domestic regulatory measures for digital trade, where it has attempted to promote digital trade, achieve high productivity growth in its digital economy infrastructure, and provide regulatory clarity for business. For instance, Singapore's PDPA allows cross-border transfers of personal data provided that organizations ensure comparable protection and does not impose strict data localization requirements. Therefore, its domestic regulatory framework remains compatible with treaty commitments that promote cross-border data flows, such as those contained in agreements like the CPTPP and the DEPA.

[159] Association of Southeast Asian Nations, *Regional Comprehensive Economic Partnership (RCEP)* (Hanoi, 2020), ch 12 (Electronic Commerce)

Singapore has actively developed its digital economy and sought to include domestic policy priorities in its digital trade agreements. The terms referenced in the DEPA and the SADEA, such as smart innovation, digital identity, and emerging technologies like AI, all echo elements of the domestic policy that underpins Singapore's broader ambitions in the digital economy. The interplay between domestic regulatory frameworks and cooperation modules in FTAs and DEAs are found in several sectors. The NAIS 2.0 and the Model AI Governance Framework for Generative AI are examples of the domestic regulatory framework for the cooperation on AI in the UKSDEA and the EU–Singapore Digital Partnership respectively. The Payment Services Act 2019 is another instance where Singapore made relevant commitments on digital payments in its DEAs which is supported by the domestic regulatory framework. The Electronic Transactions Act 2010 is the domestic legal basis for the provisions on electronic transactions found in many treaties. Nonetheless, Singapore's treaty practice is evolving to offer sufficient scope for regulation. For instance, many of its agreements contain reservations for public policy reasons.

The way Singapore approaches digital trade is partly linked to its general digital policy, which is about trying to connect the national digital economy development agenda to the international economic governance system through the WTO. In the negotiations at the WTO, Singapore is pushing forward with its digital economy development agenda, which includes promoting digital innovation, expanding digital trade, and so on, to achieve the goal of making Singapore a global-level digital economy hub, while also safeguarding its national regulatory affairs.

Policy Domain	Domestic Framework	Treaty Provisions	Alignment
Data protection	PDPA (2012, amended 2020): regulates collection, use, disclosure of personal data by private organizations; enables cross-border data flows subject to comparability safeguard	CPTPP Art. 14.8; DEPA; SADEA; UKSDEA: data protection provisions and safeguards	Aligned
E-commerce / Electronic transactions	Electronic Transactions Act (ETA) 2010: provides legal recognition for electronic contracts, records, and signatures	DEPA Art.; SADEA Art. 8; UKSDEA Art. 8: legal validity of electronic contracts	Aligned
Data localization	No blanket data localization mandate; PDPA cross-border transfers subject to adequacy safeguard	CPTPP Art. 14.13; DEPA; SADEA; UKSDEA: prohibition on localization requirements	Aligned
Cross-border data flows	Permitted under PDPA comparability framework; no general free-flow restriction	CPTPP Art. 14.11; DEPA Art. 4.3; UKSDEA Art. 8: binding free-flow obligations	Aligned

Cybersecurity	Cybersecurity Act 2018: critical information infrastructure protection; centralised governance under CSA	DEPA; UKSDEA; SADEA: cybersecurity cooperation provisions	Aligned
AI governance	NAIS (2019); NAIS 2.0 (2023); Model AI Governance Framework (2019, updated 2024 for GenAI); AI Verify	DEPA Module 8; KSDPA; UKSDEA: AI governance cooperation; EU–Singapore Digital Partnership: AI test-beds	Aligned
Digital payments / Fintech	Monetary Authority of Singapore (MAS) regulatory sandbox; Payment Services Act (PSA) 2019 licensing payment service providers	SADEA: online payment provisions; MOU on electronic invoicing	Aligned
Source code protection	No dedicated domestic provision; aligned with treaty norms	CPTPP; DEPA; UKSDEA: source code protection provisions	Aligned
Digital infrastructure & innovation	Smart Nation Initiative; DEFA; JS-SEZ digital economy focus	DEPA: digital innovation provisions; SADEA MOUs on emerging tech	Aligned

Table 4.12.2 - Domestic Digital Policy vs Treaty Provisions: Comparative Overview

4.13. South Africa

The digital policy and treaty practice of South Africa is development-oriented. South Africa has a strong domestic regulatory framework; however, there are limited treaty commitments. Domestically, the country prioritizes digital public infrastructure, service delivery, and inclusive development rather than market liberalization. However, South Africa has not adopted a standalone digital trade agreement, and the existing agreements, like the Mozambique-United Kingdom Economic Partnership Agreement (2019), contain minimal digital provisions. Despite this, it is also important to note that its participation in the DTP shows a gradual shift toward deeper digital integration. The overall relationship between the domestic policies and treaty commitments is evolving, domestic policies influence the treaty practice, and the country is beginning to maintain a balance between integration and sovereignty.

A. Domestic Digital Policy Framework

South Africa features as one of only 15 developing countries that have a mature digital economy regulatory framework with significant FDI presence in digital sectors in the WIR 2025.[160]

[160] United Nations Trade and Development (UNCTAD), *World Investment Report 2025: International Investment in the Digital Economy* (1st ed, United Nations Research Institute for Social Development 2025) 32.

South Africa's domestic digital reform is central to the Roadmap for the Digital Transformation of Government (2024/2025), a whole-of-government strategy administered through an Interministerial Committee on Digital Transformation chaired by the Minister of Communications and Digital Technologies. The Roadmap based on Operation Vulindlela (the government's flagship structural reform program) frames digital transformation as a developmental and service-delivery imperative rather than a market-opening exercise.[161] It is structured around four shared Digital Public Infrastructure (DPI) initiatives: a functional digital identity system, a real-time inter-governmental data exchange platform, a modernized digital payments infrastructure, and a single zero-rated trusted digital channel for government services. This roadmap draws explicitly on the experiences of India, Brazil, and the UK in building DPI at scale, signaling that South Africa's domestic reform is calibrated for international best practices.

The *National Artificial Intelligence Policy Framework (2024)* constitutes South Africa's first step toward a National AI Policy, organized around nine strategic pillars including digital infrastructure, research and innovation, ethical AI, privacy and data protection, safety, and transparency.[162] The framework calls for alignment of South Africa's AI governance with international norms and standards, which shows that domestic AI governance is being constructed with awareness of international regulatory trajectories, creating an internal drive toward treaty engagement that does not yet have a corresponding treaty expression.

The foundational data governance instrument is the Protection of Personal Information Act 4 of 2013 ('POPIA'), enforced in 2021. POPIA conditions cross-border data transfers on the adequacy of protection in the receiving jurisdiction, a conditional flow regime rather than a blanket localization mandate.[163] The DTI Database confirms this characterization, scoring South Africa positively on data protection framework, DPIA and DPO requirements, conditional flow regime, and the absence of a local storage requirement, which puts South Africa in the regulatory middle ground between blanket localization and unconditional free flow. The Electronic Communications and Transactions Act 25 of 2002 ('ECTA') provides the e-commerce and electronic transactions

[161] UNCTAD WIR 2025

[162] 'South_Africa_Roadmap_for_the_Digital_Transformation.Pdf' <https://stateofthenation.gov.za/assets/downloads/South_Africa_Roadmap_for_the_Digital_Transformation.pdf> accessed 25 April 2026.

[163] South Africa National Artificial Intelligence Policy Framework (2024) <https://fwblaw.co.za/wp-content/uploads/2024/10/South-Africa-National-AI-Policy-Framework-1.pdf> accessed 17 March 2026.

legal framework and expressly prohibits compelled disclosure of cryptography trade secrets, a norm that is consistent with modern digital trade governance.[164]

Year	Instrument	Type
2020	Cybercrimes Act 19 of 2020	Domestic law
2021	POPIA fully enters into force (1 July 2021)	Domestic law
2021	SACUM-UK EPA enters into provisional application (January 2021)	Treaty
2024	National Artificial Intelligence Policy Framework	Domestic policy

Table 4.13.1 Timeline of Key Domestic and Treaty Instruments

B. Treaty Practice in the Digital Sphere

South Africa's digital treaty commitments are considerably thinner than the domestic policy framework suggests. South Africa has not concluded a standalone digital trade agreement and its IIA practice has not prioritised dedicated digital chapters or digital-investment-specific provisions. The relevant agreements within the past five years are the SACU and the SACUM-UK EPA, the DTP, and South Africa's participation in the JSI.

The SACUM-UK EPA, signed in 2019 and applied in 2021, is a rollover of the pre-existing EU-SADC EPA, concluded to preserve trade continuity following Brexit, with trade in goods as its primary function.[165] The EPA does not contain a digital trade chapter: it lacks provisions on cross-border data flows, data localization, source code protection, and electronic authentication. Its digital governance dimension is confined to a development cooperation annex listing ICT as a priority area and TRIPS-derived intellectual property provisions. As an IIA, the SACUM-UK EPA therefore contributes minimally to the substantive governance of digital investment.

The DTP, adopted at the 37th AU Assembly in 2024, is the most substantively ambitious digital instrument to which South Africa is a party. It covers eleven thematic areas including market access, digital products, data governance, consumer and business trust, digital inclusion, and

[164] 'Protection of Personal Information Act 4 of 2013 | South African Government' <https://www.gov.za/documents/protection-personal-information-act> accessed 25 April 2026.
[165] 'Electronic Communications and Transactions Act [No. 25 of 2002]' <https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf> accessed 25 April 2026.

emerging technologies with eight supplementary annexes still under negotiation.[166] OECD INDIGO simulations project that full DTP implementation could raise South Africa's digital trade integration score from 0.143 to 0.589 out of 1.0 ,a 313% improvement, with the largest gains in data governance and digital identity where prior international commitments did not exist. South Africa also participates in the JSI on e-commerce, but has notably opposed the WTO e-commerce moratorium, signalling that it retains the view that the right to apply customs duties on digital transmissions should remain available as a future industrial policy option.

Policy Domain	Domestic Framework	Treaty Provisions	Alignment
Data protection	POPIA (2013/2021): adequacy-based; regulates public/private processing; independent Regulator	SACUM-UK EPA: no binding data protection disciplines; AfCFTA DTP: data governance, cross-border transfers annex under negotiation	Partial
Data localization	POPIA s 72: no blanket localization; 2024 Cloud Policy: security data stored domestically	SACUM-UK EPA: silent on localization; AfCFTA DTP limits unjustified localization; public policy exception	Tension
Cross-border data flows	POPIA s 72: permits outflows with comparable protection; no adequacy list yet	SACUM-UK EPA: no explicit data flow commitments; AfCFTA DTP: cross-border data transfers annex pending; JSI moratorium opposed	Partial
Source code / algorithms	ECTA s 29(4): protects cryptography trade secrets; pre-dates modern norms	SACUM-UK EPA: no source code provision; AfCFTA DTP: Source code annex under negotiation (CPTPP-style expected)	Aligned
E-commerce regulation	ECTA (2002, as amended): e-contracts, signatures, data messages; consumer protection	SACUM-UK EPA: ICT only in Development Annex; AfCFTA DTP: E-transactions and digital trade facilitation	Partial
AI governance	National AI Policy Framework (2024): ethical, human-centred; aligned with international standards	SACUM-UK EPA: silent on AI; AfCFTA DTP: emerging tech annex under negotiation; no binding AI rules	Gap
Digital infrastructure	Roadmap for Digital Transformation of Government (2024/25): four DPI initiatives (digital identity, data exchange, digital payments, central services channel); Operation Vulindlela	SACUM-UK EPA: ICT cooperation in Development Annex; AfCFTA DTP: facilitation & capacity building; no infrastructure obligations	Partial

[166] SACU and Mozambique–United Kingdom Economic Partnership Agreement (signed October 2019, provisionally applied 1 January 2021) (UNCTAD IIA Navigator) <https://investmentpolicy.unctad.org/international-investment-agreements/treaties/treaties-with-investment-provisions/4946/sacu-and-mozambique---united-kingdom-epa-2019-> accessed 17 March 2026.

Cybersecurity	Cybercrimes Act 19 of 2020 (in force Dec 2021): offences, decryption orders, mandatory reporting	SACUM-UK EPA: no cybersecurity chapter; AfCFTA DTP: cybersecurity annex under negotiation	Partial
Investment in digital sectors	No dedicated digital FDI promotion policy; POPIA + 2024 Cloud Policy create compliance burden for foreign investors	SACUM-UK EPA: investment chapter does not address digital-sector specifics; AfCFTA DTP: excludes government procurement; no investment promotion disciplines	Gap

Table 4.13.2 Domestic Digital Policy vs Treaty Provisions: Comparative Overview

C. Domestic Law - IIA Interaction

The WIR 2025 recommends proactive alignment of IIAs with domestic digital strategies, noting that countries with mature digital economy frameworks attract more digital FDI.[167] In South Africa's case, the domestic framework has substantially shaped the IIA commitments the country can accept; the reverse influence is currently limited but latent. The domestic-IIA interaction in South Africa can be analysed in both directions.

The most significant linkage is in data governance. POPIA's adequacy-based approach to cross-border data transfers has made South Africa's domestic framework structurally compatible with the DTP's data governance provisions, which prohibit unjustified localization requirements without mandating unconditional free flow.[168] The DTI Database's classification of South Africa under a conditional flow regime, distinct from both blanket localization and unconditional free flow, confirms that the domestic regulatory position occupies precisely the middle ground that the DTP provisions contemplate. POPIA created the domestic policy space in which the DTP data governance architecture could be accepted without legal conflict.

[167] 'The AfCFTA Digital Protocol | International Institute for Sustainable Development' <https://www.iisd.org/articles/policy-analysis/afcfta-digital-protocol> accessed 25 April 2026.

[168] 'Data Protection Laws in South Africa - Data Protection Laws of the World' <https://www.dlapiperdataprotection.com/index.html?t=law&c=ZA> accessed 25 April 2026.

ECTA's prohibition on compelled disclosure of cryptography trade secrets equally illustrates the domestic-to-treaty pipeline.[169] By embedding this protection since 2002, ECTA pre-aligned South Africa's domestic framework with the source code protection norms now being negotiated in the DTP's source code annex and already found in agreements such as the CPTPP. The WIR 2025 Toolkit confirms that effective trade secret and IP protection is a key investment climate determinant for digital multinational enterprises, suggesting that ECTA's long-standing norm has been functioning as a de facto investment facilitation measure. A domestic statute predating the modern digital trade era has thus pre-shaped the space of treaty commitments South Africa can accept, and made the eventual DTP source code annex an opportunity for international codification of an already-settled domestic norm.

The National AI Policy Framework's explicit commitment to aligning with international AI standards creates an internal pull toward digital treaty engagement, while its substantive pillars on data governance, transparency, and human-centred AI set the normative baseline against which future AI-related treaty provisions, whether under the DTP's emerging technologies annex or in a future bilateral agreement, will be assessed. This mirrors a dynamic identified by Dimitropoulos, namely that domestic policy maturity in digital industrial policy increasingly drives the content of international investment rules, rather than the reverse.[170]

The influence of IIA commitments on domestic policy is currently weak but growing. The SACUM–UK EPA has generated no measurable domestic regulatory feedback because its digital provisions are entirely cooperation-oriented rather than binding. The DTP, by contrast, has strong prospective feedback potential. Once in force, its data localization prohibition will set an upper bound on any future South African localization policies that would conflict with treaty obligations. The DTP's source code annex, once finalised, may similarly constrain the range of technology sovereignty policies available domestically, a tension that will require careful management, particularly in light of South Africa's industrial policy commitments.

[169] United Nations Trade and Development (UNCTAD), 'World Investment Report 2025: International Investment in the Digital Economy' (United Nations Research Institute for Social Development 2025) <https://unctad.org/system/files/official-document/wir2025_en.pdf>.

[170] Georgios Dimitropoulos, 'Industrial Policy and the New Internationalism'.

South Africa's opposition to the WTO e-commerce moratorium can be read in this light as a pre-emptive effort to preserve domestic policy space before treaty commitments narrow it. This is consistent with the position of scholars who observed that developing countries increasingly use treaty architecture as a site of contestation over the rules governing digital trade rather than simply as a mechanism for liberalization.

The WIR 2025 notes that digital inclusion, MSME support, and capacity-building which are considered to be the development-focused provisions are globally scarce in treaties regulating the digital economy. However, The DTP is a notable exception and South Africa's domestic developmental orientation has influenced its insistence on retaining these provisions in the Protocol. This is an example of the reverse pipeline at work: the Roadmap that focuses on inclusive public-sector digitalization has imported developmental logic into treaty architecture. This ensures that the DTP's governance framework reflects liberalization objectives and also the inclusive growth imperatives that is central to South Africa's domestic digital reform agenda.

The treaty depth of South Africa is limited as compared to some WIR 2025 top-15 peers, particularly Singapore which has signed multiple standalone DEAs with binding digital trade disciplines. The WIR 2025 recommendation that countries should align their IIAs with domestic digital strategies suggests that South Africa needs to improve and expand their agreements to close this gap as the DTP annexes are developing and future trade deals are negotiated. The goal is to ensure the domestic digital transformation is supported by international agreements.

4.14. Thailand

The digital policy in Thailand is primarily driven by an economic transformation agenda, through the Digital Economy and Society Development Plan and Thailand 4.0, whereby it prioritizes innovation, creation of a trusted digital environment, and digital infrastructure. This is further complemented by privacy, data protection, and cybersecurity laws. The model adopted allows for cross-border data flow, subject to adequate protection standards that reflect a cautious and regulated approach rather than a fully liberal one. Internationally, Thailand's treaty practice in the digital realm focuses mainly on e-commerce facilitation, cooperation, and regulatory compliance; its commitments are mainly best endeavors rather than strictly binding obligations, such as those seen in the CPTPP.

A. Domestic Digital Policies

Thailand's domestic digital policy can be best described as an economic transformation project rather than just an e-government or telecoms agenda. Under the Thailand Digital Economy and Society Development Plan (the 'Plan'), digital technology is presented as the key mechanism for national development, and the plan states that the country must "urgently adopt digital technology as an important growth engine" for services, production, trade, and public administration.[171] The vocabulary frequently used in the Plan is quite revealing and is framed around "*competitiveness*", "*transformation*", "*prosperity, stability, and sustainability*", and the construction of "*Digital Thailand*", framing Thailand as a state that is capable of using innovation, human capital, and its infrastructure for national development. This approach aligns comfortably with the Thailand 4.0 agenda, which connects technological and digital development to higher value-added production as well as participation in global value chains.[172]

The Plan's framework emphasizes trust and infrastructure development. For example, Strategy 1 of the Plan calls for "countrywide high-efficiency digital infrastructure", and it seeks to position the country as an ASEAN hub for "connectivity and data exchange". Importantly, Strategy 6 of the plan is titled "*Build trust and confidence in the use of digital technology*" and is pertinent for domestic-treaty analysis as it states that Thailand needs standard rules, laws, and policies that are "*efficient, up to date, and in line with international norms*", with a specific focus on cybersecurity and personal data and privacy protection. This policy approach is further reinforced through legislation. The Cybersecurity Act 2019, which defines cybersecurity maintenance in national security and broader public order terms, and establishes a centralized governance model through a national committee chaired by the Prime Minister.[173] It is important to note that the language used is security-driven and protective. Similarly, the Electronic Transaction Act also supports transactional trust through digital identity verification systems.

The data governance model is quite cautious compared to a pure free-flow model. For example, under section 28 of the PDPA, transferring personal data abroad must, in principle, go to a

[171] Ministry of Digital Economy and Society, Thailand Digital Economy and Society Development Plan (May 2016) 1–2
[172] Ministry of Industry, Thailand 4.0 policy (official policy document) 1–3
[173] Cyber Security Maintenance Act, BE 2562 (2019) ss 3–5

destination with "*adequate data protection standards*", unless an exception is afforded.[174] Although this is not a classic case of data localization, it is not an unconditional free flow of data and is closer in structure to regulated transfer rather than to blanket liberalization. Indeed, the recent implementing notifications in 2023 and 2024 were specifically designed for this purpose, namely to operationalize sections 28 and 29 for cross-border transfers.[175]

B. Thailand's Treaty Practice in the Digital Sphere

The treaties in discussion in this section are the following:

(1) The Free Trade Agreement between the EFTA States and the Kingdom of Thailand;
(2) the RCEP;
(3) the CPTPP;
(4) the ASEAN; and
(5) the ATISA.

Thailand's treaty practice is embedded in regional ASEAN instruments, service agreements, and FTAs rather than being centered on a stand-alone digital economy agreement. Although this approach demonstrates a mixed pattern, it is coherent. For example, agreements such as the RCEP and the ASEAN Agreement on Electronic Commerce provide detailed electronic commerce chapters, and in particular, the RCEP's chapter uses language that evidently shows to what extent Thailand is willing to. It states that the main objective is to "contribute to creating an environment of trust and confidence in the use of electronic commerce" and enhance cooperation in global trade and e-commerce.[176] This is strikingly similar to the language used in the domestic policies, namely, Strategy 6 of the Plan.

However, hard obligations are approached cautiously when looking into Thailand's treaty practice. For example, the RCEP does not adopt strong language in its treaty text as seen in the CPTPP, namely, the CPTPP states that each Party "*...shall allow cross-border transfer of information by electronic means*" and "*...shall not require a covered person to use or locate computing facilities*"

[174] Personal Data Protection Act BE 2562 (2019) s 28, official English text
[175] Personal Data Protection Committee notifications on cross-border transfers under ss 28–29, discussed in Tilleke & Gibbins, 'Thailand Unveils Regulations for Cross-Border Personal Data Transfer' (4 January 2024)
[176] Regional Comprehensive Economic Partnership Agreement (signed 2020, in force 2022) ch 12 art 12.2

in its territory, with narrow public policy exceptions.[177] The ASEAN and other agreements often use softer, best endeavor formulations. For example, the ASEAN agreement on Electronic Commerce provides that Member States "*... recognise the importance of allowing information to flow across borders through electronic means*" and "*...agree to facilitate cross-border e-commerce… by working towards eliminating or minimising barriers*".[178]

Although in services and financial data provisions, the ATISA's financial services annex provides that a Member State "*...shall not take measures that prevent transfers of information, including transfers of data by electronic means, necessary for the conduct of the ordinary business of a financial service supplier*", it immediately preserves the states right to protect personal data, confidentially, and personal privacy of individual records and accounts and extends this to even allow regulators for prudential reasons to require compliance with domestic laws on data management, local retention of copies of records, and storage.[179] Furthermore, the regulatory chapter to the ATISA also provides that Member States "*...shall endeavour to accept applications in electronic format*" and "*...to the extent possible*", make relevant measures available "*on the internet*".[180] It is evident here that the language used is not that of hard digital market access; rather, it is facilitative, while not deeply constraining.

C. Domestic Law – IIA Interaction

Broadly speaking, a closer comparison of Thailand's domestic digital policies and its treaty practice shows that they reflect rather than constrain its domestic regulatory priorities. First, the strong emphasis on digital infrastructure development and technological adoption is reflected in treaty provisions that promote paperless trade, connectivity, and the facilitation of e-commerce. For example, the Plan emphasizes nationwide broadband infrastructure and a digital economic transformation, and several ASEAN agreements also include commitments that encourage the use of electronic documentation and digital trade systems.

---

[177] Comprehensive and Progressive Agreement for Trans-Pacific Partnership (signed 2018, in force for Thailand not applicable) arts 14.11 and 14.13.

[178] ASEAN Agreement on Electronic Commerce (signed 2019, in force 2021) art 7(4)(a)–(b) and art 7(6) (pages 9–10 of the treaty text).

[179] ASEAN Trade in Services Agreement (signed 2020, in force 2021) Annex on Financial Services art 9.

[180] ASEAN Trade in Services Agreement ibid art 14(3) and art 16(9).

Second, Thailand's treaty practice substantially preserves regulatory flexibility, which is in line with the country's domestic governance model. As observed, the Cybersecurity Act places particular emphasis on national security and economic stability considerations in regulating digital systems, and the same is evident in treaty provisions addressing cross-border data flows that often include exceptions that allow the local government to adopt measures necessary for the protection of public policy objectives (i.e., national security, privacy, cybersecurity).

Lastly, unlike the European Union's ('EU') digital agreements, which harmonize regulatory standards, Thailand's treaties do not strongly export a specific regulatory model in the way the EU often does. Rather, it appears to adapt its commitments to regional frameworks, for example, the ASEAN agreements. In those agreements, the language used frequently emphasizes dialogue, information sharing, and cooperation rather than strict harmonization of regulatory standards.

4.15. Türkiye

Türkiye is more cautious about international agreements and has a state-led model of digital development. Domestically, Türkiye prioritizes sovereignty, digital infrastructure development, and the updating and support of its own industry. Their legal framework is very controlling of data governance, but allows cross-border data flows subject to safeguards. This cautiousness is also evident in its treaty practices, which include provisions on electronic transactions, paperless trade, and cooperation, but avoid commitments on cross-border data flows, data localization, or source code protection. The interaction between its domestic and international commitments suggests that Türkiye preserve regulatory autonomy and support domestic capacity building.

A. Domestic Digital Policy Framework

Türkiye has many development-oriented digital policies and laws, including those related to industrial strategy, AI, data governance, digital infrastructure, and e-commerce regulation. Therefore, viewing digitization as a tool for economic development.

The Twelfth Development Plan (2024-2028) aims to increase productivity and strengthen industrial competitiveness and includes provisions on digital infrastructure. The 2023 Industry and Technology Strategy and the broader National Technology Initiative, on the other hand, focus on the goal of technological sovereignty, domestic production, and innovation capacity. These

policies aim to strengthen Türkiye's domestic technological capabilities by promoting research and development and encouraging domestic manufacturing in high-tech sectors to reduce dependence on foreign technologies.

Türkiye's National AI Strategy (2021-2025) focuses on improving access to data and technical infrastructure, promoting AI research and innovation, supporting workforce transformation, and establishing governance mechanisms for AI. The Turkish National E-Science E-Infrastructure (TRUBA), on the other hand, promotes high-performance computing and large-scale data processing. Additionally, initiatives such as the Türkiye Open-Source Platform and the Open Data Project promote domestic software development and data accessibility.

On its legal framework, Law No. 6698 on the Protection of Personal Data (2016) establishes the country's data governance model and regulates the processing and transfer of personal data. This law allows cross-border data transfers (with safeguards) and has a controlled approach to data flows. Commentary suggests the recent amendments of the law attempt to "*harmonize with European legislation*".[181]

The Electronic Signature Law (Law No. 5070 of 2004) provides legal recognition for electronic signatures and facilitates digital transactions. Additionally, Law No. 6563 on the Regulation of Electronic Commerce governs digital market activities and includes obligations on online platforms. Türkiye is also cautious on digital finance as its Regulation on the Disuse of Crypto Assets in Payments prohibits the use of crypto-assets in payment services.

Year	Instrument	Type
2004	Law 5070 (Electronic Signature)	Domestic law
2016	Law 6698 (Personal Data Protection Law)	Domestic law
2021	Regulation on Crypto Assets in Payments	Domestic law
2021	National AI Strategy (2021-2025)	Domestic policy
2023	Türkiye-UAE CEPA	Treaty
2023	Türkiye-Qatar TEPA	Treaty
2024	Twelfth Development Plan	Domestic policy

Table 4.15.1 Timeline of Key Domestic and Treaty Instruments

[181] Esin Attorney Partnership, 'Amendments to the Turkish Data Protection Law' (12 March 2024) https://www.esin.av.tr/2024/03/12/amendments-to-the-turkish-data-protection-law/ accessed 13 April 2026.

B. Treaty Practice in the Digital Sphere

Recent agreements indicate that Türkiye is engaged with digital trade governance while also maintaining a cautious and selective approach. The agreements examined include:

(1) the Türkiye-UAE Comprehensive Economic Partnership Agreement ('CEPA');

(2) the Trade and Economic Partnership Agreement between the Republic of Türkiye and the State of Qatar ('TEPA'); and

(3) the JSI.

The Türkiye-UAE CEPA has a Digital Trade Chapter that establishes rules governing electronic transactions and digital trade and recognizes the legal validity of electronic transactions and signatures. For instance, Article 9.6(1) states that, except otherwise provided in its law:

> *"...a Party shall not deny the legal validity of a signature solely on the basis that the signature is in electronic form."*

Additionally, Article 9.6(2)(a) further provides that parties shall not:

> *"...adopt or maintain measures regarding authentication that would prohibit parties to an electronic transaction from mutually determining the appropriate authentication methods for that transaction."*

The agreement also has provisions on paperless trading. Article 9.7 provides that the Parties shall endeavor to make trade administration documents available in electronic form and accept electronic documents as legally equivalent to paper documents. Clear, however, is the soft wording on this and many provisions of the agreement.

Consumer protection and data governance are also addressed, as Article 9.9(2) states that:

> *"Each Party shall adopt or maintain a legal framework that provides for the protection of the personal data of the users of digital trade."*

However, the agreement does not impose strong obligations regarding cross-border data flows. Article 9.12 states that:

> *"The Parties recognise the importance of the flow of information in facilitating trade and acknowledge the importance of protecting personal data."*

This is clearly cautiously worded, as although it recognizes the importance of data flow, there is no binding obligation to ensure it. The agreement also makes no mention of prohibiting data localization and contains no provisions on source code protection. TEPA also contains provisions relevant to digital trade, though in a more limited scope, as the agreement focuses on trade facilitation and the use of electronic means in commercial activities. For instance, the agreement promotes paperless trading. In Article IV.8, it states that:

> *"The Parties shall endeavour to accept trade administration documents submitted electronically as the legal equivalent of the paper version of those documents."*

Additionally, the agreement includes provisions encouraging cooperation between the Parties in areas related to trade facilitation and the use of digital technologies, as set out in Article IV.9. However, like CEPA, TEPA does not include provisions on cross-border data flows, data localization restrictions, or source code protection. Türkiye's involvement with the JSI shows that, in some way, the country wants to be involved with shaping or being part of emerging digital trade norms; however, other than its participation in the JSI, this desire is not shown elsewhere. It must be noted that the JSI is not a strict or hard law; as such, Türkiye's participation does not bind it to its regulations.

Overall, Türkiye's treaty practice is consistent in containing certain digital provisions while remaining cautious and limited on other, more liberal provisions, such as cross-border data flows and the prohibition of localization.

Policy Domain	Domestic Framework	Treaty Provisions	Alignment
Data protection	Law 6698 regulates personal data	CEPA Art. 9.9(2); TEPA limited	Partial
Data localization	Controlled transfers	No explicit treaty restriction	Partial
Cross-border data flows	Allowed with safeguards	CEPA Art. 9.12 (non-binding)	Gap
E-signatures	Law 5070	CEPA Art. 9.6; TEPA recognition	Aligned
E-commerce	Law 6563	Both agreements include provisions	Aligned

Digital infrastructure	Strong domestic policy	Weak treaty reflection	Gap
AI governance	National AI Strategy	Minimal treaty reference	Gap
Trade facilitation	Strong digital gov framework	TEPA paperless trade provision	Aligned
Cybersecurity	Domestic policy	CEPA cooperation provisions	Partial

Table 4.15.2 - Domestic Digital Policy vs Treaty Provisions: Comparative Overview

C. Domestic Law – IIA Interaction

Comparing Türkiye's domestic digital policies with its treaty practices, it is clear that both are relatively protective and prioritize the Turkish economy. Domestically, Türkiye prioritizes technological development, digital infrastructure, and regulatory control. This is also reflected in its treaties through provisions that support electronic transactions, digital trade facilitation, and cooperation. Furthermore, its treaties are not particularly liberal, as they avoid obligations regarding cross-border data flows and data localization. This also reflects Türkiye's domestic approach, which allows digital development while maintaining regulatory oversight. TEPA is almost the same as CEPA in terms of its degree of liberalization; however, compared to CEPA, TEPA is more limited and focuses primarily on cooperation and facilitation rather than on binding commitments.

5. Development Dimension

5.1. Defining Development-Oriented Provisions in IIAs

The main takeaways from the preceding analysis of 77 IIAs across 15 countries is that development-oriented provisions in IIAs in relation to the digital economy remain scarce and limited in both scope and substance. In assessing their prevalence or absence, it is important first to define what are "*development-orineted provisions*" in an operational sense; this is particularly important when discussing this in the context of the digital economy, whereby the connection between investment, development, and technology transfer is inherently more complex to navigate than in more traditional sectors. It is widely recognised that the majority of IIAs do not in a systematic way address the role of investment in advancing digital development goals, but rather

are designed for an analogue economic environment, namely, a business model revolved around physical, traditional, and non-digital processes[182].

For the purposes of this report, development-oriented provisions are defined as treaty provisions that exceed the traditional objectives of investment protection and liberalization. Rather, development-oriented provisions seek, in a sense, to facilitate domestic capacity building, equitable participation in the digital economy, and restructuring. This definition flows from the general conceptualization of investment policy for sustainable development by UNCTAD, whereby it emphasises the need for IIAs to not only protect investors but also contribute to the host-state development objectives and results[183]. Particular attention is required for technological asymmetries, regulatory capacity constraints, and infrastructure in the digital context, as these aspect shape the ability of developing countries to benefit from digital investments.

To operationalise this definition, identification of specific categories of provisions that could be systematically coded throughout the dataset was required . First, a core indicator of development orientation was *technology transfer provision*s as they include provisions that either encourage or mandate the transfer of knowledge, innovation capabilities, and technical expertise between both the host-state and investors. Traditional IIAs did not include such provisions and were relatively rare or framed in best-endeavour, non-binding language. However, where such provisions do appear, such as in the AFCFTA which explicitly refers to promoting technology and knowledge transfer, they signal a recognition that investment should objectively contribute to domestic technological upgrading[184]. Second, capacity-building and technical assistance was also considered in the analysis, namely, regulatory frameworks, human capital, and strengthening domestic institutions. Such provisions are extremely significant in the digital economy context as participation in the digital markets is heavily dependent on regulatory competent and skilled labour, not only on infrastructure. These provisions can be frequently found in cooperation chapters and can include obligations to regulatory dialogue and institutional support such as training programs. The Indonesia–United Arab Emirates Comprehensive Economic Partnership

[182] Georgios Dimitropoulos, 'Investment Law and the Digital Economy' (2025) 16 *Journal of International Dispute Settlement*, 1-2. See generally Rodrigo Polanco, 'The Impact of Digitalization on International Investment Law: Are Investment Treaties Analogue or Digital?' (2023) 24 German Law Journal 574.
[183] UNCTAD, *Investment Policy Framework for Sustainable Development* (UN 2015).
[184] *Protocol to the Agreement Establishing the African Continental Free Trade Area on Investment* (adopted 2023) arts 28, 30, and 31-33.

Agreement (2022), for example, contain commitments to cybersecurity cooperation referring particularly to workforce development and institutional capacity[185].

Third, a distinct category identified was digital infrastructure provisions which focus on the development of telecommunications networks, digital connectivity, and data infrastructure. Although traditional IIAs do not frequently address infrastructure directly, recent agreements incorporate cooperation mechanisms with an objective to facilitate investment in the digital sector and improve digital connectivity. Fourth, the analysis also included provisions related to SMEs and digital inclusions; such provisions recognise that the benefits of digital trade and investment are unevenly distributed and that SMEs face participation barriers in digital trade. The United Kingdom–Singapore Digital Economy Agreement (2022), for example, contains provisions that address SME participation directly and include linking digital trade governance to broader development goals and digital inclusion[186]. It is important to note that not all cooperation or soft-law provisions were categorised as development-oriented, the approach in the report critically distinguishes between development specific provisions and cooperation clauses. For example, cooperation clauses using "*endeavour to cooperate*" in the digital economy without reference to mechanisms, areas of intervention, or beneficiaries were not categorised as development-oriented for the purposes of this report.

The definition approached in this report reflects a shift in the concept of development in international investment law. Traditional IIAs treated development as an indirect outcome of investment, however, the realities of the digital markets and economy challenge this. Investment in relation tot he digital economy remain highly concentrated in a limited number of advanced agreements and economies around the world, without targeted policy intervention[187]. Development oriented provisions, albeit limited and uneven, is an attempt to align investment governance with more binding and explicit objectives. However, their presence across the 15 countries remains sporadic and where they do appear, are framed in best-endeavour language and aspirational terms.

---

[185] *Indonesia–United Arab Emirates Comprehensive Economic Partnership Agreement* (signed 1 July 2022) ch 9 (Digital Trade), art 9.13.

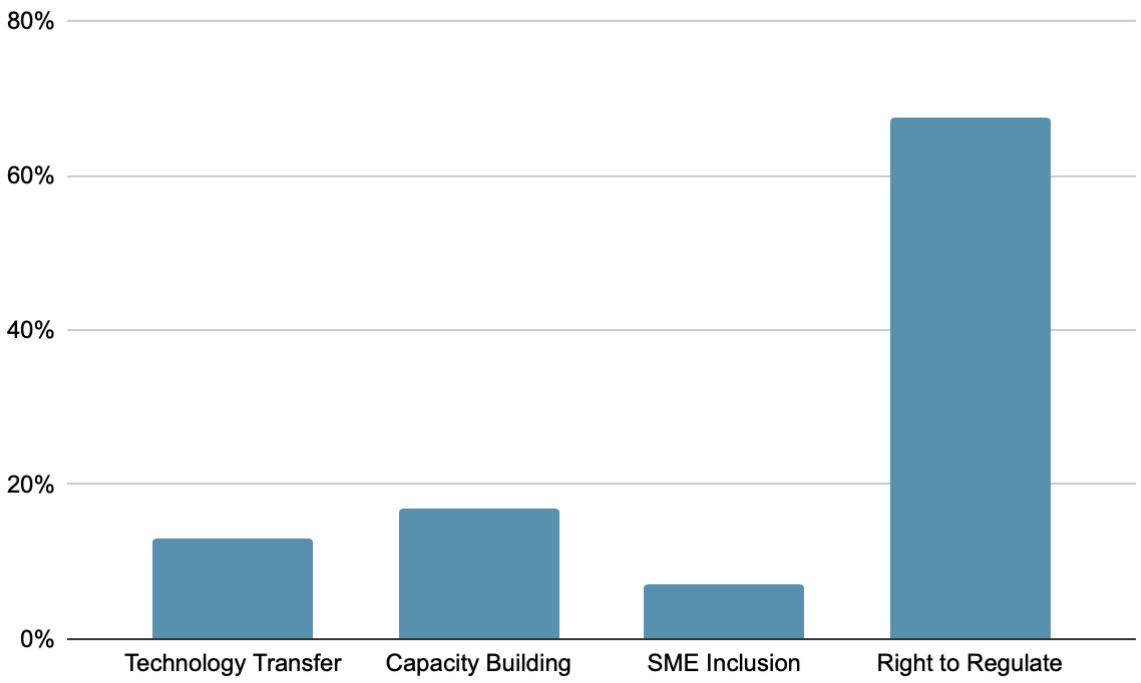
[186] *United Kingdom–Singapore Digital Economy Agreement* (signed 10 December 2020, entered into force 14 June 2022) chapter on Digital Inclusion and Cooperation.

[187] UNCTAD, *World Investment Report 2025: International Investment in the Digital Economy* (UN 2025).

5.2. Empirical Findings

The mapping exercise provides an insight on the extent to which development-oriented provisions are included in IIAs across the 15 country dataset. Although such provisions do exist, they remain limited in scope and substance and are distributed unevenly across regions and types of agreements. The mapping exercise confirms that only 13% of sampled agreements contain explicit provisions relating to technology transfer provisions, fewer than 7% address digital inclusion or MSME support, and capacity-building and technical assistance provisions appear in under 17% of agreements.[188] By contrast, right-to-regulate clauses appear in 67.5% of sampled IIAs, indicating that states prioritize preserving policy space over embedding affirmative development commitments. The current scarcity underscores the urgent need for more development-sensitive digital frameworks to serve the interests of the Global South and foster inclusive digital development.

[188] See Section 3.3 above; of the 77 agreements mapped, only 10 (13.0%) contain explicit technology transfer provisions.



Graph 5.1: Prevalence of Development-Oriented Provisions

Category	% of Agreements	Interpretation
Dedicated Digital Chapter	40.3%	Moderate uptake but concentrated in few countries
No Digital Provisions	45.5%	Large share still “analogue-era”
Technology Transfer	13%	Very limited and mostly soft-law
Capacity-Building / Technical Assistance	<17%	Present but weakly institutionalized
SME / Digital Inclusion	<7%	Almost absent

Right to Regulate	67.5%	Dominant provision (defensive approach)

Table 5.2.1: Prevalence of Digital & Development-Oriented Provisions (77 IIAs)

An additional important finding is the significant variation between the different types of agreements, namely development-oriented provisions are highly likely to be found in the "*new-generation*" trade agreements and regions treaties, especially those with a dedicated digital chapter. For example, the AfCFTA framework is somewhat distinctive: its Digital Trade Protocol promotes and incorporates explicitly and direct references to digital inclusion and supports MSMEs, while its Investment Protocol requires investments to make notable progress in sustainable development and shields regulatory measures from compensation claims. Nonetheless, eight annexes are still being negotiated, with full implementation anticipated by 2029. AfCFTA demonstrates that development-sensitive treaty structures can be feasible, but it remains an exception, as most bilateral and regional agreements have not followed similar strategies. Similarly, the the Indonesia–United Arab Emirates CEPA, and the United Kingdom–Singapore Digital Economy Agreement also promote and incorporate direct and explicit references to inclusion, cooperation and capacity building. When comparing those examples to tradition BITs (such as the Mexico-United Arab Emirates BIT) within the mapping exercise, the development-oriented provisions are overwhelmingly scarce and focus instead on core investment protection clauses for example such as fair and equitable treatment and expropriation.

The mapping exercise also reveals that development-oriented provisions, where prevalent, are formulated mainly as non-binding obligations such as best-efforts framed typically in terms such as "*the Parties shall endeavor to cooperate…*" specifically in relation to technology transfer, capacity-building. Although such clauses reflect awareness of the development dimensions in this context, they remain limited in their practical impact. Such provisions are also largely confined to the agreements that adopt a general economic partnership approach. The AfCTRA Investment Protocols does recognise the importance of infrastructure and development and signals awareness but frames such commitments in more programmatic terms rather than impactful and enforceable

terms[189]. In relation to SME participation and digital inclusions, the exercise reveals again concentrated in a limited small subset of digital economy agreements. For instance, the United Kingdom–Singapore Digital Economy Agreement (2022) incorporates provisions that address barriers to participation in the digital economy whereby parties commit to cooperate in facilitating access to digital tools, skills, and supporting SME engagement, however, although such provisions recognise the uneven participation, they are yet framed as cooperation commitments and do not provide enforceable rights or obligations on parties[190]. The mapping exercises also reveals that many of the development-oriented provisions are frequently incorporated in agreements separately from the core investment disciplines, namely, rather than being recognised and embedded within binding investment obligations, such provisions are typically found in ancillary sections or cooperation chapters, limiting integration into the broader agreement framework. li

Development Need	Does domestic policy often address it?	Treaty practice addresses it?	Gap
Digital infrastructure	Yes	Partially	Medium
Skills / human capital	Yes	Weakly	High
SME inclusion	Sometimes	Rarely	Very High
Technology transfer	Sometimes	Rarely	Very High
Data governance capacity	Yes	Partially	Medium
Investor contribution to development	Rarely	Rarely	Very High

Table 5.2.2 - Development Gap Matrix

Country	Technology Transfer	Capacity-Building	SME / Inclusion	Digital Infrastructure	Overall Development Orientation
Armenia	None	Low	None	Low	Low
Brazil	Low	Low	None	Medium	Low
Colombia	Low	Low	None	Low	Low

[189] *Protocol to the Agreement Establishing the African Continental Free Trade Area on Investment* (adopted 19 February 2023) art 30; arts 31–33.

[190] *Digital Economy Agreement between the United Kingdom of Great Britain and Northern Ireland and the Republic of Singapore* (signed 25 February 2022, entered into force 14 June 2022) chapter 8 on Digital Economy Cooperation, inclusion and SME participation.

Costa Rica	Low	Medium	Low	Low	Low–Medium
Kenya	Medium	Medium	Low	Medium	Medium
Mexico	None	Low	None	Low	Low
Nigeria	Low	Low	None	Low	Low
Pakistan	Low	Low	None	Low	Low
Peru	Low	Low	None	Low	Low
Rwanda	Medium	Medium	Low	Medium	Medium
Saudi Arabia	Low	Medium	Low	High	Medium
Singapore	Low	Medium	Medium	Medium	Medium–High
South Africa	Medium	Medium	Low	Medium	Medium
Thailand	Low	Low	None	Low	Low
Türkiye	Low	Medium	Low	Medium	Medium

Table 5.2.3 - Country-Level Intensity of Development-Oriented Digital Provisions in IIAs

5.3. The Direction of Influence: Domestic Policy and Treaty Interaction

A central finding of the country's case studies concerns the direction of influence between domestic digital policies and IIA commitments. Three patterns emerge.

First, where domestic frameworks are aligned with treaty disciplines, states accept those disciplines without conflict - and often without requiring domestic legislative reform. Armenia's DPL (2015) and its decision not to impose blanket data localization requirements enabled it to engage with both the CEPA and EAEU frameworks without tension. Kenya's DPA (2019) established a conditional flow regime that proved structurally compatible with the AfCFTA DTP's data governance provisions. Rwanda's electronic transactions legislation (Law No. 18 of 2010) provided the domestic foundation for continental requirements on electronic contracts and digital identities. In each case, prior domestic regulatory development created the conditions for treaty acceptance. Such a pattern suggests development-oriented domestic regulation can be a precondition for, rather than an obstacle to, international economic integration.

Second, the direction of influence is predominantly international-to-domestic for many developing countries, but the content of that influence varies significantly across treaty partners. Mexico's

digital policy frameworks have evolved amid its integration into North American supply chains. For context, the USMCA's digital chapter has shaped Mexican domestic digital governance, rather than the other way around. Thailand's treaty practice reflects ASEAN frameworks rather than a distinctive national regulatory model. By contrast, Singapore has used its treaty practice to project its domestic digital governance model internationally through standalone Digital Economy Agreements, creating a pattern of domestic-to-international influence that developing countries have not replicated.

Third, several countries demonstrate a 'regulate first, negotiate second' strategy that preserves development policy space. Rwanda built strong domestic regulatory institutions before engaging in continental negotiations, enabling it to enter AfCFTA discussions from a position of institutional strength. Saudi Arabia's domestic digital policy framework, including the PDPL, NCA cybersecurity controls, and NSDAI, was developed largely autonomously, driven by Vision 2030's economic diversification imperatives rather than by external treaty obligations. Brazil's selective stance on treaty commitments (namely, embracing digital economy rules that promote innovation but avoiding those that might limit industrial and technological goals) demonstrates strategic flexibility. This approach helps maintain policy space for developing the domestic digital industry.

These patterns suggest that the relationship between domestic digital policies and IIA commitments is not zero-sum. Countries with more mature digital economy frameworks are better positioned to shape treaty rules rather than simply adopt them as rule-takers. The order of actions is important: strengthening domestic regulatory capacity before committing to binding treaties seems to increase, rather than reduce, negotiating leverage.

Category	Countries	Explanation
Rule-exporting model	Singapore	Domestic digital governance is projected into treaty practice
Regulate-first model	Rwanda, Saudi Arabia, Brazil, Kenya	Domestic frameworks precede or shape treaty engagement
Rule-importing model	Mexico, Thailand, Armenia	Treaty practice reflects external/regional models
Low treaty-development model	Nigeria, Pakistan, Peru, Colombia, Costa Rica	Domestic or treaty practice contains limited development-oriented commitments

Mixed / strategic model	Türkiye, South Africa	Selective engagement with digital provisions while preserving policy space

Table 5.3.1 - Country Development-Orientation Typology

	Low treaty development depth	**High treaty development depth**
High domestic maturity	Brazil, Saudi Arabia, Türkiye	Singapore, Rwanda, Kenya
Low / emerging domestic maturity	Nigeria, Pakistan	Costa Rica, Peru, Colombia

Table 5.3.2 - Domestic Maturity vs Treaty Development Depth

5.4. Answering the Research Questions

What is the place of digital economy provisions in IIAs? Digital provisions remain unevenly distributed: 40.3% of mapped agreements contain a dedicated digital chapter, while 45.5% contain none. Coverage is concentrated among a few active treaty-makers (Singapore accounts for half of all dedicated chapters). Where digital provisions appear, they predominantly address liberalization (data flows, localization restrictions) rather than development (technology transfer, inclusion).[191]

What is the link between domestic frameworks and IIA provisions? The link is asymmetric: every country studied has domestic strategies more advanced than treaty coverage. Direction of influence varies by capacity - Singapore exports its model; Mexico and Thailand import external templates; Rwanda, Saudi Arabia, and Brazil built domestic capacity first. Although Mexico's domestic digital policy has evolved to reflect the disciplines of that of the USMCA, for example, no instance was found where treaty provisions have directly driven domestic digital development policy.[192]

What is the role of digital development in these frameworks? Development occupies a marginal place. Affirmative provisions (technology transfer, inclusion, MSME support) appear in fewer than 17% of agreements, typically as soft cooperation and best-endeavor language. The

[191] See Section 3.2 above.

[192] See Sections 4.1–4.15 above for detailed country analysis/channeling.

AfCFTA is exceptional in combining development provisions with enforceable disciplines. For most developing countries, IIAs function as constraints on policy space rather than instruments advancing development objectives. The role of development is to protect existing spaces through right-to-regulate clauses, rather than actively directing investment towards inclusive change.

5.5. Implication for Policymakers

The findings of this report provides insights as to the current treaty practice, namely, that it is not yet equipped to support digital development goals in a more effective and systematic manner. Moreover, although development-oriented provisions are emerging frequently in newer agreements, they still remain limited in scope, are structurally marginal to core investment disciplines, and are weak in their enforceability. Addressing this weakness or gap, will not be achievable merely through treaty reform alone, and requires a shift from viewing development as an indirect result of investment agreements, to treating development as an explicit goal of the overall treaty design. The most effective approach is to ensure treaty commitments do not foreclose development policy options while building domestic foundations that enable engagement from a position of strength. The WIR 2025 confirms that countries with mature digital frameworks attract more digital FDI; maturity is built domestically before being signaled internationally.[193] Further, this approach is aligned with UNCTAD's general investment policy framework, which stresses the need to ensure investment governance alignment with sustainable development goals[194]. This section will provide practical implications for policymakers to consider and will propose effective approaches to embedding development considerations into IIAs in digital markets and digital economies.

First, it is recommended that there be a move beyond broad cooperation provisions and more towards specific and operational development provision, namely, presently as observed in agreements such as the Indonesia–United Arab Emirates Comprehensive Economic Partnership Agreement and the United Kingdom–Singapore Digital Economy Agreement, such provisions often rely on best-endeavour language without any measurable obligations. In the Indonesia-UAE CEPA Article 9.13, for example, references cybersecurity cooperation and includes training and

[193] UNCTAD, World Investment Report 2025: International Investment in the Digital Economy (United Nations 2025) 212–214.
[194] UNCTAD, *Investment Policy Framework for Sustainable Development* (UN 2015).

capacity-building but through best-efforts language rather than binding commitments[195]. Similarly, Chapter 8 of the UK-Singapore Digital Economy Agreement also address SME participation and inclusion but through voluntary cooperation[196]. A consideration therefore, would be to draft such provisions with clearly identifying beneficiaries, mechanisms, as well as areas of intervention. Second, development considerations need to be embedded and considered in IIAs as core investment disciplines, rather than incorporating development-oriented provisions in ancillary sections or confining them to cooperation chapters. As observed, when comparing the traditional BITs to AfCFTA Investment Protocol, such provisions are more effective when integrated in the agreement's broader structure. This can be found for example, in the Protocol to the Agreement Establishing the African Continental Free Trade Area on Investment in Articles 30 on transfer of technology and Articles 31-33 on investor obligations, directly linking investment activity to the development goals[197]. It is recommended for policymakers to consider incorporating development provisions that directly link investment activity and protection with explicit contribution commitments to domestic development outcomes.

Third, the mapping exercise illustrates that institutional capacity-building and infrastructure is a critical constraint for developing countries, and policymakers should strongly consider strengthening infrastructure and capacity-building provisions that become central to achieving meaningful participation in digital markets and the digital economy. This is recommended to be approached through detailed commitments and obligations that support infrastructure, human capital, and regulatory cooperation; more specifically, particular attention should be given to more detailed commitments such as joint infrastructure initiatives, training programs and skills development, and technical assistance for domestic actors and authorities. This can also be done through building on existing frameworks and cooperation models that are limited in that respect, for example, such as those found and observed in the Indonesia-UAE CEPA agreement. Fourth, to address digital inclusion and SME participation, policymakers should consider to operationalise inclusion and participation by strengthening the programmatic features of such provisions and

[195] *Indonesia–United Arab Emirates Comprehensive Economic Partnership Agreement* (signed 1 July 2022) art 9.13.
[196] *Digital Economy Agreement between the United Kingdom of Great Britain and Northern Ireland and the Republic of Singapore* (signed 25 February 2022, entered into force 14 June 2022) ch 8.
[197] *Protocol to the Agreement Establishing the African Continental Free Trade Area on Investment* (adopted 19 February 2023) art 30; arts 31–33.

introduce more specific measures that facilitate SME access to the digital economy and digital markets more broadly, namely, financing and access to critical digital platforms.

Finally, a more systematic approach is recommended to better achieve these results in relation to treaty design whereby development policy objectives align with specific legal and enforceable mechanisms. Namely, the recommended treaty design that is development-oriented will require alignment with the broader treaty structure, and not merely the inclusion of such isolated provisions; more embedded and integrated approaches are feasible, for example as observed in the AfCFTA Investment Protocol, however these remain limited in practice presently. Structural and substantive reform is required to achieve these outcomes.

6. Conclusion

This report reviews 77 IIAs across fifteen countries and highlights three main findings that are relevant for reforming investment law in the digital age.

First, digital provisions are now part of treaty practice, but their distribution remains uneven and concentrated in a limited number of agreements and treaty-makers. About 40% of the agreements include a digital chapter, while nearly 46% have no digital content at all. Rules on data - cross-border data flow obligations (33.8%), data localization restrictions (16.9%), and source code protections (15.6%) - appear only in a small number of agreements. These are mostly used by a few digitally advanced countries, especially Singapore. Overall, most existing treaties reflect a pre-digital economy that has not yet adapted.

Second, the relationship between domestic digital policy and treaty commitments is uneven across the sample. In the 15 countries studied, domestic frameworks are found to be more developed than treaty coverage. Three patterns can be observed: a domestic-to-international model, illustrated by Singapore; an international-to-domestic model, illustrated by Mexico and Thailand; and a regulate-first approach, illustrated by Rwanda, Saudi Arabia, Brazil, and Kenya. The direction of influence is important for policymakers. Countries that develop domestic regulatory capacity before entering binding treaty commitments are better placed to shape those commitments in line with national development objectives.

Third, development-related provisions are limited. Technology transfer provisions appear in 13% of the mapped agreements, digital inclusion and MSME support in fewer than 7%, and capacity-building commitments in under 17%. By contrast, right-to-regulate clauses appear in 64.9% of agreements, showing that existing IIAs focus more on preserving policy space than on directing investment towards development outcomes. The AfCFTA Digital Trade Protocol and Investment Protocol provide partial exceptions to this, but the overall pattern across the dataset remains clear.

To conclude, future treaty design should move beyond this defensive approach. Development-oriented provisions should be integrated into the main investment disciplines rather than placed in cooperation sections, made operational through specific commitments with defined beneficiaries and mechanisms, and treated as core treaty objectives rather than secondary aims.

Annex

The following link is to a copy of the working document in our IIA digital repository, which lists the IAAs we have researched for this project in an Excel sheet.

https://docs.google.com/spreadsheets/d/13kbF43bm6_b6ff0W6obSSmtkA2J7TzEXuy0tuNYIsRM/edit?usp=sharing