Policy Research Journal
ISSN (E): 3006-7030 ISSN (P) : 3006-7022 Volume 3, Issue 12, 2025

DATA REGULATIONS AND DIGITAL SOVEREIGNTY: A NEW CHALLENGE TO INTERNATIONAL INVESTMENT LAW

Dr. Ali Nawaz Khan[*1], Israr Ahmad[2], Dr. Bakht Munir[3]

[*1]*Assistant Professor of Law, University Law College, University of the Punjab, Lahore*
[2]*LLM Scholar, University Law College, University of the Punjab, Lahore*
[3]*Postdoc Fellow, The University of Kansas School of Law, USA*

[*1]alinawaz.law@pu.edu.pk, [2]israrshahoor@gmail.com, [3]bakht.munir@ku.edu

DOI: https://doi.org/10.5281/zenodo.18115183

Keywords
Data localization, digital sovereignty, Foreign Direct Investment, International Investment Law, cross border data flows

Article History
Received: 11 October 2025
Accepted: 21 November 2025
Published: 31 December 2025

Copyright @Author
Corresponding Author: *
Dr. Ali Nawaz Khan

Abstract
With the rapid expansion of the digital economy, states have increasingly sought to assert digital sovereignty through the enactment of new data regulations. These include data-localization requirements, restrictions on cross-border data flows, and comprehensive privacy frameworks, all aimed at safeguarding national security, protecting individual privacy, and supporting domestic industries. Governments—most prominently within the European Union, China, and other jurisdictions—conceptualize digital sovereignty as the capacity to act autonomously in the digital sphere or to exercise control over their digital destiny. Yet, such measures inevitably intersect with the principles of international investment law, requiring scrutiny by foreign investors and arbitral tribunals. This paper examines the tensions between sovereign data-control policies and treaty-based investment protections, providing background on the evolution of multi-layered digital regulation and situating these developments within the broader framework of international economic law.

1. INTRODUCTION

The accelerating shift toward a digital economy has compelled many states to reassess the strategic importance of data and technology within their economic policies. Increasingly, governments pursue digital sovereignty through legislative measures designed to assert or preserve jurisdiction over data generated within their territories. At one end of the spectrum, some scholars conceptualize digital sovereignty as the general right of a state to regulate and control the flow of information across its jurisdiction (Svantesson, 2019). The European Parliament defines digital sovereignty as Europe's capacity to act independently in the digital sphere, emphasizing both protectionist measures and the pursuit of innovative policy (Organisation for Economic Co-operation and Development [OECD], 2020). In practice, aspirations for digital sovereignty have given rise to a diverse array of regulatory instruments, including data-localization laws mandating the domestic storage or processing of specific datasets, compulsory data-security and privacy frameworks, and restrictions on cross-border

data transfers justified on grounds of national security or privacy protection (Raza, Munir, Ali, Othi, & Hussain, 2024). Notably, more than thirty-four countries—including major economies such as Germany, Russia, China, Brazil, and Malaysia—have adopted some form of data-localization requirement (Zhang & Mitchell, 2022). States frequently justify these measures as essential for safeguarding cybersecurity, enabling effective law enforcement, protecting individual privacy, and enhancing economic competitiveness (Cory & Dascoli, 2021).

At the same time, international investors have consistently expected unrestricted market access through international investment agreements (IIAs). These agreements—often structured as bilateral investment treaties (BITs) or embedded contractual guarantees within broader trade frameworks—are designed to secure protections against discrimination, ensure fair and equitable treatment (FET), and safeguard foreign investors from uncompensated expropriation. Traditionally, however, IIAs were drafted in an era when the term *asset* referred primarily to tangible infrastructure such as factories, mines, or foreign enterprises, rather than the intangible exchanges of information or digital services that dominate today's economy (Khan, Munir, & Ahmed, 2020). As Georgios Dimitropoulos observes, contemporary international investment agreements (IIAs) were designed to address the needs of a traditional economic environment and contain few provisions specifically tailored to the digital economy (European Parliament, 2025). Similarly, Rodrigo Polanco argues that international investment agreements (IIAs) "are not intended for the digital era," though their typically broad definitions may incidentally encompass investments in data-intensive sectors (Polanco, 2023). Today, investment projects are increasingly reliant on cross-border data flows, encompassing cloud services, telecommunications networks, e-commerce platforms, and artificial intelligence applications (Munir, 2025). Digital regulations, therefore, present a twofold challenge to international investment law. First, such policies can undermine the legitimate expectations of investors; for example, mandatory data-localization requirements or compelled transfers of technology and data may disrupt the business models of foreign enterprises. Second, these measures may conflict directly with treaty obligations, raising questions of compliance under international investment agreements. The proliferation of multi-layered digital governance illustrates this tension: at the domestic level, states increasingly adopt data-localization mandates, compulsory data-sharing rules, and investment-screening mechanisms; at the international level, new trade agreements such as the CPTPP and USMCA incorporate chapters on digital governance, while commentators advocate for the negotiation of entirely new treaties designed for the digital era (Hepburn, 2017).

This paper investigates the intersection between data-sovereignty regulations and international investment law. It raises three central questions: to what extent do data-localization measures and related policies conflict with fundamental protections under international investment agreements (IIAs)? How can arbitral tribunals adjudicate disputes in which data itself constitutes the contested asset? And what reform options might reconcile these tensions? The analysis focuses on doctrinal issues—treaty texts, case analogies, and comparative approaches across jurisdictions—while also suggesting pathways for future development. The paper is structured as follows: Section II clarifies the key concepts of digital sovereignty and data localization; Section III examines the requirements of international investment law and assesses whether data-related measures fall within its scope; Section IV provides comparative insights from major economies such as China, the European Union, and the United States; and Section V proposes reforms, including treaty amendments and the establishment of multinational guidelines, aimed at aligning investment law with contemporary data governance.

Defining Digital Sovereignty and Data Regulations

Before analyzing the legal implications, it is essential to clarify the key terminologies. *Digital sovereignty*—along with related concepts such as *data sovereignty* and *technological sovereignty*—is generally understood as a state's assertion of authority to control data, technology, and associated economic activities within its territorial jurisdiction (Oliver Wyman, 2021). Recent analyses suggest that the concept of digital

(cyber/information) sovereignty can be understood as the ownership of one's digital destiny—that is, control over the data, hardware, and software upon which individuals and states depend and which they produce. Scholars, however, caution that such terminology is often employed without sufficient precision. An OECD report, for instance, notes that terms such as *data sovereignty*, *information sovereignty*, and *digital sovereignty* are frequently invoked but rarely defined with clarity or grounded in established principles of international law (Voss, 2020). For example, early conceptualizations of information sovereignty—developed in the 1970s and reflected in Soviet doctrine—asserted that a state held the prerogative to control all internal streams of information. This approach stood in sharp contrast to Western notions favoring the free distribution of information. In its contemporary application, however, digital sovereignty is often understood to encompass both defensive and creative dimensions. The European Union, for instance, defines digital sovereignty not only in terms of protective mechanisms but also as a framework for fostering digital innovation.

Data localization—also referred to as data residency—denotes a legal obligation requiring certain data to be stored or processed within the jurisdiction of a specific country. According to an OECD study, data-localization requirements are mandates imposed through legal or administrative measures that compel data to remain within national borders. These obligations can take various forms. Some laws prohibit the cross-border transfer of particular categories of data, such as personal information or data related to critical infrastructure, thereby requiring such data to be retained domestically or restricting its processing abroad. Others adopt a non-exclusive approach, permitting cross-border transfers subject to specific conditions, such as government access rights or compliance with encryption standards. Additional localization measures may arise from procurement rules or industry-specific legislation, including cybersecurity laws that mandate the domestic storage of government-related or sensitive data (European Commission, 2024). More importantly, localization initiatives are frequently embedded within broader regulatory frameworks, including digital-surveillance legislation, cybersecurity laws, and privacy regimes. For the purposes of this analysis, the term *data regulation* (or *data rule*) is employed in a broad sense to encompass localization requirements, restrictions on cross-border data flows, mandatory data-sharing obligations with government authorities, and related measures.

This segment analyzes the implications of data-regulation measures for international investment law. In this context, *investment* refers to any asset covered by an investment treaty, typically including shares, contracts, intellectual property rights, and other privileges associated with business enterprises. The generation or processing of data by a foreign-owned enterprise, or through its assets, can therefore qualify as an investment protected under prevailing treaty frameworks. Indeed, treaty definitions of investment frequently encompass intellectual property and other forms of property owned by foreign investors, thereby extending protection to data-driven activities (Ahmed, Munir, & Khan, 2021). It is important to note that arbitral tribunals have already recognized intangible and contractual rights as protected investments. For instance, in *CC/Devas v. India*, a contract allocating satellite spectrum was deemed a covered investment. By analogy, contracts or licenses granting investors the right to collect, use, or manage data within a host state can similarly fall within the scope of treaty protection. Moreover, the entire business operations of a foreign corporation—such as those of a cloud-services provider—may qualify as an investment, with the underlying data assets constituting a significant source of value (Rudolf & Schreuer, 2012). Overall, foreign investments have increasingly relied on cross-border data flows and digital services. In this regard, Chaisse and Bauer contend that "digital assets" fall within the scope of bilateral investment treaties (BITs) and examine the extent to which security- and privacy-related measures might be defended under BIT provisions((Chaisse & Bauer, 2019).

Since data-generating activities may qualify as investments under international investment treaties, and given that data regulations can significantly affect such investments, it is assumed that the customary treaty protections apply. These include guarantees of national treatment (equal treatment of

foreign and domestic investors), most-favoured-nation (MFN) treatment, the duty of fair and equitable treatment (FET—commonly understood as stability and protection of legitimate expectations), and safeguards against both direct and indirect expropriation. In addition, many treaties prohibit performance requirements, such as conditioning investment on technology transfer, local-content obligations, or other mandated business practices. The central question, therefore, is how modern data regulations fit within this framework. For instance, can a data-localization requirement be interpreted as a prohibited performance requirement—since it dictates the geographic location of data infrastructure—or as a violation of national treatment, insofar as it imposes disproportionate burdens on foreign firms compared to domestic ones? These are the issues that will be addressed in the following analysis.

Data Laws with International Investment Law

This section examines the intersection between data-regulation measures and the fundamental provisions of international investment treaties. The analysis focuses on key IIA standards, including non-discrimination (national treatment), most-favoured-nation (MFN) treatment, fair and equitable treatment (FET), expropriation, performance requirements, and dispute-resolution mechanisms, and considers how data-localization mandates or related state actions may conflict with these protections. A further question arises regarding the definition of *investment* itself, and whether data can be regarded as an investment asset under treaty frameworks. In the absence of direct precedent—since no investor-state award has yet been determined specifically on data-related laws—the discussion draws upon analogous treaty clauses and arbitral cases to identify potential pathways of interpretation.

Localisation of Data and Treatment at the National Level

A traditional provision of investment treaties is that host states must not discriminate against foreign investors in comparison with domestic investors (the national-treatment requirement), nor among foreign investors themselves (the MFN requirement). Data-localization measures, however, often produce discriminatory effects. For example, a policy requiring data generated in country X to be stored on servers located within X may be easily complied with by local firms that already maintain domestic data centers, but it imposes significant costs on foreign firms reliant on global networks. A localization law that disproportionately burdens foreign investors can therefore amount to a breach of national treatment. Scholars have noted that mandatory data-storage requirements confer competitive advantages on local companies at the expense of foreign enterprises. Zhang and Mitchell (2022) argue that data-localization measures are detrimental to foreign investment, enhance the economic benefits available to domestic firms, and ultimately contravene the principle of national treatment under international investment agreements (Zhang & Mitchell, 2022). This study further concludes that the legality of a data-localization measure, insofar as it implicates national-treatment obligations, depends on the specific treaty language and the availability of security or public-order exceptions within the IIA. Absent such explicit exceptions, a government may struggle to justify a localization rule that imposes unequal treatment on foreign and domestic businesses. Consequently, classical discrimination-based claims may arise. For instance, a foreign investor could argue that, while a local competitor is permitted to transfer data to a foreign cloud provider, the investor is compelled to retain data domestically—constituting unequal treatment under the treaty framework.

On the other hand, certain IIAs and related trade agreements now expressly prohibit data-localization requirements. Notably, recent trade-investment frameworks such as the CPTPP and USMCA contain dedicated digital-economy chapters that outlaw localization commitments. For example, CPTPP Article 14.13 provides: *"No Party shall require the use or location of computing facilities in that Party's territory as a condition for conducting business in that territory."* (Comprehensive and Progressive Agreement for Trans-Pacific Partnership [CPTPP], 2018, art. 14.13(2)) Similarly, USMCA Article 19.12 adopts the same approach, stipulating 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."* This provision,

like CPTPP Article 14.13, reflects a deliberate effort to prevent data-localization mandates from becoming barriers to trade and investment, thereby reinforcing the principle of non-discrimination in the digital economy (Bian, 2023). These provisions articulate a clear policy against digital protectionism, prohibiting states from introducing localization requirements that disadvantage foreign investment. Although the terminology varies across agreements, the underlying pattern is unmistakable: recent treaties consistently promote the free movement of data across borders and seek to prevent disguised forms of discrimination (Microsoft Corp v. India, 2019). By contrast, older IIAs lack explicit provisions addressing data-localization, and similar disputes would therefore be resolved under more general treaty standards, such as national treatment (NT) or most-favoured-nation (MFN) clauses ((Khan, Munir, & Jawwad, 2020).

The Fair and Equitable Treatment and Expropriation

Fair and Equitable Treatment (FET) and expropriation are critical standards that safeguard investors' rights to legitimate expectations and due process. A data-regulation measure may breach FET if it is arbitrary, discriminatory, or unfairly deprives investors of anticipated benefits. For example, if a foreign company enters a market with the expectation of freely transferring user data, only to find that such transfers are suddenly prohibited, the company could claim a violation of FET or denial of justice due to unfair procedures. Similarly, an indirect-expropriation claim may arise where a localization requirement effectively strips proprietary data or software of its economic value—whether by obliging its destruction or rendering it unusable. In such cases, tribunals typically assess factors such as the degree of deprivation and the investor's legitimate expectations (see *Salini* and related jurisprudence). Although data is intangible, arbitral practice has consistently recognized non-physical assets—including networks, patents, trademarks, and spectrum licenses—as protected investments. By analogy, critical data infrastructure and data-related rights may also fall within the scope of treaty protection.

Although no investor-state award has yet directly addressed a dispute centered exclusively on data-localization, useful analogies can be drawn from established cases. For instance, in *CC/Devas v. India*, the arbitral tribunal recognized telecom spectrum licenses—together with the associated contracts—as protected investments, even though these assets primarily conferred rights to manage information flows. This precedent suggests that intangible rights linked to data transmission and infrastructure may likewise be treated as covered investments under international investment law (Khan, Munir, & Jawwad, 2020). By analogy, datapipes or datasets may be regarded as intangible property within the meaning of investment definitions. Where a localization statute or forced data-processing requirement substantially eliminates investor control over such assets, claims of indirect expropriation or breach of Fair and Equitable Treatment (FET) may be viable. At the same time, states often invoke regulatory grounds to justify such measures: public-interest objectives relating to health, security, or privacy are typically permitted under narrowly construed exceptions and necessity defenses, and many IIAs contain implicit exceptions for essential security or public order. As Zhang and Mitchell observe, the legality of data-localization requirements often turns on whether the IIA expressly or implicitly authorizes state action to protect essential security interests, public order, or public morals (Zhang & Mitchell, 2022). In practice, a localization rule introduced as a cybersecurity measure may fall within the scope of an exception, provided it is formulated in sufficiently broad terms. Absent a specific exception, however, tribunals are likely to inquire whether the measure was genuinely necessary and applied in a non-discriminatory manner.

Performance Requirements

Data-localization requirements can be analogized to performance requirements under investment treaties. Most BITs, following the precedent set by NAFTA and similar agreements, prohibit host states from conditioning investment on the forced transfer of technology, production processes, or source code. Although data is not explicitly mentioned, localization mandates—such as obligations to use local servers or processing facilities—can be compared

to performance requirements insofar as they impose operational conditions on foreign investors. For example, CPTPP Article 14.17 expressly forbids requiring the transfer of software source code as a condition for market entry, illustrating how modern treaty provisions seek to prevent states from imposing such burdensome requirements on investors (United Nations Conference on Trade and Development [UNCTAD], 2021). This reflects a broader trend: contemporary treaties are increasingly restrictive of attempts to condition market access on the transfer of digital assets. By contrast, older IIAs relied on generic "no performance requirement" clauses, which could arguably be interpreted to bar localization measures. For instance, NAFTA Article 1106 prohibits technology-transfer requirements, a provision that in certain contexts might encompass restrictions on data flows. Nevertheless, because localization rules are typically justified on non-economic grounds—such as security or privacy—the applicability of these clauses remains debatable. To date, such provisions have seldom been directly tested in relation to data measures. However, if a localization requirement were construed as a disguised method of compelling technology (or data) disclosure or nationalization, an investor could plausibly argue that it violates the performance-requirement prohibitions contained in a BIT.

Investor-State Dispute Settlement (ISDS)

One of the major distinctions between trade law and Investor-State Dispute Settlement (ISDS) lies in their procedural design. Whereas trade disputes are resolved on a state-to-state basis, international investment agreements (IIAs) empower individual investors to initiate claims directly against host states that fail to comply with treaty obligations (UNCTAD, n.d.; Khan, Munir, & Jawwad, 2020). Any violation of investment obligations arising from data-related measures may entitle the affected investor to damages through arbitration, for example under ICSID, UNCITRAL, or similar institutions. While trade agreements typically envisage state-to-state dispute settlement, bilateral investment treaties (BITs) provide investors with direct remedies against host states. To date, no arbitral awards have been issued specifically on data-localization, but tribunals may soon confront such cases. Recent studies suggest that data-related investment disputes are likely to emerge as a new frontier in arbitration, particularly in fast-growing economies with extensive data-regulation regimes. Put simply, the risk of ISDS underscores that data regulation is not merely a matter of domestic legislation; incompatibility with treaty guarantees may expose states to costly international litigation.

Definition of Investment and Data

At a certain stage, it becomes necessary to consider whether data itself qualifies as an investment under treaty law. Most IIAs adopt a broad definition of investment, encompassing "every kind of asset," including movable and immovable property, equity shares, and intellectual property rights. Within such expansive formulations, there is a strong doctrinal basis to argue that data—particularly when structured as proprietary datasets, databases, or digital infrastructure—may fall within the scope of protected investment assets (Ramesh, 2018; Ahmed, Munir, & Khan, 2021) Although raw data is not explicitly mentioned in investment treaty definitions, it can be subsumed under broader categories of protected assets. Digital content, algorithms, and databases may be classified as intellectual property or other forms of property derived from data. Accordingly, when a foreign investor establishes or operates data centers, networks, or AI frameworks in a host state, such enterprises are secured as investments, with the associated data forming part of their property base. Recent scholarship on emerging sectors—including space data—supports this view, noting that arbitral tribunals have already safeguarded telecommunications infrastructure contracts and patents as investments. By analogy, critical data assets and infrastructures may similarly fall within the protective scope of IIAs (Chander & Lê, 2015). Moreover, academics speculate that data services derived from space activities could also fall within the ambit of investment protection. Thus, while the pure concept of data—namely, simple flows of information—may be regarded as a borderline case, investments premised on data, and in some instances even data-based products themselves, are generally considered to fall within the scope of treaty protections.

Overall, data-regulation measures can give rise to traditional investment claims. A localization requirement, for instance, may be challenged on grounds of discrimination, amounting to a breach of the national treatment (NT) standard. Depending on its design and application, such a measure could also implicate most-favoured-nation (MFN) obligations, Fair and Equitable Treatment (FET), or even indirect expropriation if it substantially deprives investors of the economic value of their data assets. In this way, disputes over data localization are not entirely novel but rather extensions of established treaty protections into the digital domain (Creach, 2020). Claims arising from data-localization measures may be framed in traditional investment law terms, including arbitrariness (breach of FET), uncompensated taking (expropriation), or unlawful performance requirements. Ultimately, the wording of the treaty—such as the scope of security exceptions—and the factual context, including considerations of public purpose and proportionality, will determine whether such claims succeed. What remains incontrovertible is that states cannot assume data lies outside the jurisdiction of investment law. Regulators must either be prepared to justify localization measures in arbitral proceedings or, more prudently, work toward the establishment of an international legal framework governing data-flow restrictions in advance, as commentators have cautioned (Kuner, 2013).

The following section provides a comparative study of how the key economies deal with data regulation and investment commitments:

China

The People's Republic of China has established a robust framework of digital sovereignty. Its **Cybersecurity Law, Data Security Law,** and **Personal Information Protection Law** (often referred to collectively as the "Chinese GDPR") impose stringent localization and security-review obligations on both personal and non-personal information. For example, critical or important personal data collected in China must generally be stored domestically and may not be transferred abroad without prior government approval.

Chinese firms themselves face restrictions on the use of foreign data services and technology transfers. These measures, however, may conflict with China's extensive portfolio of bilateral investment treaties (BITs), most of which—reflecting an early-generation paradigm—provide only general protections such as **NT, FET,** and safeguards against expropriation. As Cheng Bian has argued, China's national data-governance and sovereignty agenda is fundamentally at odds with the investor protections embedded in its IIAs, creating a structural incompatibility that increases the likelihood of investor-state disputes.

In practice, a foreign firm operating in China may expect to freely transfer data as part of its business model, yet domestic law now prohibits such transfers. Bian suggests that lawsuits involving data regulation could emerge as a new frontier for foreign investors challenging Chinese measures. Although no arbitral tribunal in China has yet adjudicated a case focused purely on data localization, BITs are currently being renegotiated, and China has signed onto several digital-economy FTAs (e.g., **RCEP** and its ongoing **CPTPP accession process),** signaling external pressure to constrain localization. The central challenge remains how Beijing will balance its technology-security imperatives with its investment-liberalization commitments.

European Union

The European Union articulates its vision of digital sovereignty primarily through strong data-protection and infrastructure policies. The **GDPR** imposes strict limitations on the movement of personal data, effectively extending EU jurisdiction over data relating to EU citizens worldwide. In the sphere of digital trade, the EU promotes the principle of **"data free flow with trust",** which supports open cross-border data transfers while safeguarding privacy. A recent example is the **EU–Japan data pact (July 2024),** which established mutual adequacy provisions to permit the free flow of personal data between the two jurisdictions, thereby eliminating arbitrary localization requirements. The EU explicitly framed this agreement as a countermeasure to digital protectionism and as part of its broader commitment to embracing economic digitalization.

In its investment treaties, the EU and its member states often include exceptions for data-related measures. For instance, the **Trade and Investment**

Chapter in CETA incorporates general security exceptions and "Carlsberg clauses" permitting public-interest regulation. However, EU treaties do not contain explicit provisions on data localization. At the same time, EU law has introduced certain localization elements: **Article 45 of the e-Commerce Directive** prohibits mandatory in-country hosting, yet national laws governing telecommunications or cloud procurement may still impose localized requirements. EU investors operating in third countries therefore encounter boundaries on host-state data obligations, as reflected in rulings by German and other courts rejecting localization demands that exceed EU law. The interaction between such domestic rulings and the protections afforded under International Investment Agreements (IIAs), however, remains largely unexplored.

United States

The United States has consistently advocated for the free flow of data, a position reflected in its trade agreements such as the **USMCA** and earlier **TPP negotiating texts**, both of which prohibit forced localization. Domestically, the U.S. has traditionally adopted a sectoral approach to data governance, relying on voluntary principles or industry-specific protections rather than comprehensive localization laws. Instead of emphasizing localization, U.S. policy frames digital sovereignty primarily through the lens of **national security,** with the maxim that "economic security is national security."

Recent developments, however, suggest a shift. In early 2025, the **Department of Justice (DOJ)** introduced regulations prohibiting U.S. companies from transferring certain categories of sensitive personal data—including biomedical and genomic data—to designated "countries of concern," such as China, Russia, and Iran (Cory & Dascoli, 2021). Although formally framed as anti-surveillance measures, these rules functionally resemble localization requirements by restricting data outflows to specific jurisdictions.

From an investment law perspective, U.S. IIAs and agreements such as NAFTA/USMCA contain general security exceptions that likely encompass such measures. Yet the extraterritorial scope of the DOJ rule—applying even to U.S. persons abroad—raises potential conflicts. For example, a European investor could theoretically challenge the rule under a U.S.–EU investment treaty if prohibited from transmitting data to a European cloud server. This remains untested in arbitral practice. Conversely, U.S. companies operating in countries with strict localization laws (e.g., China or Vietnam) may argue that such measures conflict with Chapter 11 of the USMCA or NAFTA+ provisions, which explicitly forbid localization requirements. In this sense, the American commitment to avoiding localization is reaffirmed, even as national-security-driven restrictions blur the boundary between free data flows and regulatory control.

United Kingdom

The United Kingdom, in its post-Brexit regulatory trajectory, has sought to balance continuity with innovation in the digital economy. Retaining the UK GDPR framework, it remains aligned with European privacy standards, yet recent policy initiatives emphasize flexibility to attract investment and foster growth. The government's Smart Data Roadmap illustrates its ambition to leverage data across sectors such as finance, energy, and telecommunications, while maintaining consumer trust through the oversight of the Information Commissioner's Office (ICO) (UK Government, Department for Business and Trade, 2024). At the international level, the UK has signaled interest in joining plurilateral frameworks like the Digital Economy Partnership Agreement (DEPA), positioning itself as a proactive player in shaping global digital trade rules (Organisation for Economic Co-operation and Development [OECD], 2025). Importantly, the enactment of the **Property (Digital Assets etc) Act 2025** (United Kingdom, 2025) marks a significant development: by recognizing certain digital assets, including crypto-tokens and NFTs, as property, the UK provides legal certainty for investors and expands the scope of what may qualify as protected investment under IIAs (Law Commission of England and Wales, 2023). This property-law dimension complements its broader digital-trade commitments, situating the UK as a bridge economy—less sovereignty-heavy than the EU, but more cautious than the US and Japan—seeking to reconcile openness with regulatory autonomy in the digital era.

Developing Countries

Data localization has increasingly been adopted by developing states as a means of asserting sovereignty or pursuing industrial policy. In India, for example, the government's digital strategy envisions treating data as a national resource and promoting localization, though these initiatives have not yet been fully enforced. Negotiations on a **Digital Economy Agreement with the EU** remain ongoing. By contrast, Russia has already mandated the domestic storage of personal data under **Federal Law 242-FZ**, while countries such as Vietnam and Nigeria have introduced sector-specific localization requirements.

The most common rationales for these measures include safeguarding citizens' data and fostering local cloud industries. Yet many of these states are parties to bilateral investment treaties (BITs) with Western and Asian partners, creating potential conflicts (Khan, Munir, & Ahmed, 2020). For instance, an Indian technology company investing abroad might invoke investment protections if a third country restricts information flows to India. Similarly, foreign firms in Nigeria could challenge local-content data provisions under Nigerian BITs.

The current legal environment is inconsistent. Modern treaties such as the **CPTPP, USMCA,** and the **Australia–Chile FTA** explicitly prohibit localization requirements, whereas older BITs lack such provisions. This imbalance produces an uneven regulatory platform, compelling investors to scrutinize the specific terms and conditions of each IIA before committing to cross-border digital operations.

Trade vs. Investment Instruments

It is instructive to note that contemporary trade agreements and economic frameworks have begun to take explicit positions on digital flows. In addition to the provisions contained in the **CPTPP** and **USMCA,** numerous countries are participating in the **WTO Joint Statement Initiative on E-commerce,** launched in 2019, which emphasizes the principle of **"data free flow with trust."** Although the initiative has yet to culminate in a finalized agreement, it reflects a growing multilateral effort to reconcile open cross-border data flows with privacy and security safeguards.

By contrast, there is currently no multilateral investment treaty that provides comparable guidance on data policy. Investment law remains largely silent on digital flows, with only limited references in regional instruments. For example, the **ASEAN Comprehensive Investment Agreement** addresses data issues only superficially. As Dimitropoulos observes, this situation creates multiple layers of law in practice: **domestic law** (national data-regulation regimes), **bilateral or regional law** (trade agreements or BITs), and the potential emergence of **global norms** (Dimitropoulos, 2025). The relationships between these layers continue to evolve. For instance, under the EU–Japan Economic Partnership Agreement (EPA), data-flow regulation is already applied across most industries, with only limited exceptions (Comprehensive and Progressive Agreement for Trans-Pacific Partnership [CPTPP], 2018, art. 14.13(2)). The existing data rules may influence arbitral reasoning if an EU or Japanese investor were to initiate a third-country investor-state arbitration under the investment chapter of an EPA. Yet, in the absence of express treaty provisions on data, much will depend on how arbitrators interpret the general terms of the agreement.

In short, the comparative landscape reveals significant disparity. Certain jurisdictions, most notably China and the European Union, embrace strong notions of digital sovereignty, though they pursue divergent paths: China emphasizes inward-facing data controls rooted in national security, while the EU advances a holistic framework of data-protection practices. By contrast, the United States and Japan prioritize openness, complemented by carve-outs designed to safeguard security interests.

Where these policies intersect with investment treaties, tensions inevitably arise. The prospect of investment claims in the digital domain is a relatively new development. As commentators have noted, geopolitical competition over digital governance is intensifying among the United States, China, and the European Union, with arbitration likely to become a key arena in which these rival approaches are tested (OECD, 2019). Digital sovereignty is increasingly asserting itself as concentrated technology platforms and strong-state coercive measures take hold. Within this competitive environment, investment law may evolve into a

central forum for dispute resolution—or more constructively, a negotiation platform—where the balance between open data markets and legitimate policy objectives is contested and defined.

Reform Proposals

The possibility of conflict raises the question of how investment law can be recalibrated to meet the demands of digital sovereignty. Scholars and policymakers have advanced several reform proposals.

One approach is the inclusion of **explicit treaty carve-outs.** International investment agreements (IIAs) could adopt specific language permitting regulatory measures in the field of data when justified by security, privacy, or public-order considerations. Similar to the public-morality or security exemptions frequently found in IIAs, such provisions would expressly shield reasonable data-protection policies. For example, a treaty might stipulate that interpretations of provisions within the chapters on national treatment (NT) or fair and equitable treatment (FET) do not preclude the adoption of data-localization requirements or restrictions on cross-border data flows, provided these measures are non-discriminatory and proportionate. This approach would mirror existing exceptions, such as Article 20 of the GATS or the security exceptions in NAFTA.

Recent treaty practice reflects movement in this direction. The **2022 Canada Model FIPA,** for instance, contains a clause permitting cybersecurity actions, though it stops short of expressly addressing data-flow regulation. Another strategy is the adoption of an **authority clause,** which affirms the state's right to regulate the information economy in pursuit of community interests, as suggested in OECD commentary.

Trade agreements already provide examples of acceptable localization criteria. For instance, **CPTPP Article 14.13** recognizes circumstances under which localization measures may be justified, offering a template for how investment law might evolve to accommodate digital-sovereignty concerns (Dimitropoulos, 2025). Text analogous to this, if incorporated into International Investment Agreements (IIAs), could provide more comprehensive guidance for arbitrators and policymakers in addressing data-related disputes.

Chapters of Bilateral and Regional Digital Economy

Instead of relying solely on traditional investment chapters, states are increasingly able to conclude specific digital-economy agreements. The **Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)** and the **United States–Mexico–Canada Agreement (USMCA)** already contain stand-alone digital-trade chapters that set out rules on data flows. Other frameworks, such as the **Digital Economy Partnership Agreement (DEPA)** between Singapore, New Zealand, and Chile, similarly address data flows and digital innovation.

Multilateral Frameworks or Guidelines

At a broader level, the establishment of an international agreement on data flows could significantly reduce uncertainty. This may be pursued through multilateral initiatives, such as ongoing **WTO e-commerce negotiations,** or through the creation of new international accountability mechanisms governing the cross-border movement of data. The **Cornwall Consensus program**, referenced by scholars such as Dimitropoulos, represents one vision for embedding broad-based principles of consensus into the digital economy.

Comparable discussions are taking place within the **OECD Privacy Guidelines** and the **Global Forum on Digital Trade,** both of which explore exceptions and safeguards for data governance. According to **Columbia FDI Perspectives,** policymakers could design an international legal framework for information-movement restrictions that ensures transparency, predictability, and efficiency, while also meeting public-policy objectives. One proposal suggests a **two-tier approach**: combining ongoing arbitration to resolve disputes with pre-negotiated rules that define the permissible scope of data control within agreed limits.

Treaty Practice Reform

Arbitration policies may evolve on the procedural front. Parties could agree to appoint specialists in data governance to assist tribunals, or to expedite

proceedings involving data-related measures given their technical complexity. Institutions such as the **International Centre for Settlement of Investment Disputes (ICSID)** and **UNCITRAL** could issue interpretative notes clarifying how existing treaty language applies to data concerns, thereby enhancing predictability in arbitral outcomes.

States may also revise their model Bilateral Investment Treaties (BITs). For instance, they could specify what constitutes an investment and, equally important, what does not. Explicit provisions could affirm that regulatory actions taken to protect data privacy or security do not amount to expropriation. Such clarifications would help reconcile investment protections with legitimate public-policy objectives in the digital domain.

Development Concerns

In the developing world, sovereignty is often invoked as a rationale for implementing data-regulatory frameworks. Yet these nations also rely heavily on foreign investment inflows. International aid could therefore play a constructive role in building trust—for example, by providing technical assistance to establish secure data-transfer systems and ensuring that localization policies are not driven solely by fears of exclusion.

The perceived necessity of localization may be reduced through the promotion of data-sharing agreements that incorporate strict protection standards. Stakeholders emphasize the importance of fostering inclusive dialogue, as highlighted by the OECD, to guarantee that all countries and internet actors have a voice in international discussions. Such engagement can help mitigate unilateral pressures toward localization and encourage cooperative approaches to global data governance.

Reservation of Investment Treaty

A more pragmatic, though somewhat fragmented, approach is the incorporation of reservations or non-conforming measures into International Investment Agreements (IIAs). For instance, when ratifying a treaty, a state may declare that its domestic data laws fall outside the scope of the treaty's protection provisions. This method, however, is problematic. It is frequently employed in the context of security exceptions, yet it imposes no binding obligation on future jurisprudence and leaves considerable uncertainty for arbitral interpretation.

A more effective solution would be to negotiate an additional protocol or amendment to an IIA that explicitly addresses data-related issues. Such instruments could provide clear guidance on how data regulation interacts with investment protections, thereby reducing ambiguity and aligning treaty practice with the realities of digital governance.

Conclusion

The overarching goal of reform is to reduce legal ambiguity arising from the tension between states' regulatory prerogatives over data and investors' treaty-based entitlements. A collaborative rather than adversarial approach is preferable. Rather than waiting for localization measures to be challenged before arbitral tribunals, decision-makers should act proactively at the negotiation stage. Clear treaty formulations or the adoption of new international standards can help balance legitimate public interests—such as privacy and security—with the economic benefits of open digital markets. In a world where data is often described as the "new oil," governments and investors alike must recognize its dual character: both as an economic resource and as a matter of public policy concern.

International investment law must evolve if it is to remain relevant in the digital era. Failure to manage data flows risks rendering existing frameworks obsolete. Over-protecting investors at the expense of essential data-governance measures invites political backlash and potential repudiation of treaties. The way forward lies in a middle ground: revising IIAs to include precise provisions on data policies and carefully crafted exceptions that prevent arbitrary discrimination while safeguarding core protections. A hybrid model—combining trade-style commitments on data flows with investment protections—may well represent the future architecture of digital-era agreements.

REFERENCES

Ahmed, N., Munir, B., & Khan, A. N. (2021). Intellectual property rights and economic development: A case study of Pakistan. *Journal of Historical Studies,* 7(1), 157–174.

Bian, C. (2023). Data as assets in foreign direct investment: Is China's national data governance compatible with its international investment agreements? *Asian Journal of International Law, 13*(2), 342–365. https://doi.org/10.1017/S204425132300020X

Chaisse, J., & Bauer, C. (2019). Cybersecurity and the protection of digital assets: Assessing the role of international investment law and arbitration. *Vanderbilt Journal of Entertainment & Technology Law, 21*(1), 41–86.

Chander, A., & Lê, U. P. (2015). Data nationalism. *Emory Law Journal, 64*(3), 677–739.

Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), Dec. 30, 2018, art. 14.13(2) (Location of computing facilities).

Cory, N., & Dascoli, L. (2021, July 19). *How barriers to cross-border data flows are spreading globally, what they cost, and how to address them.* Information Technology & Innovation Foundation. https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost-and-how-address-them/

Creach, M. A. (2020, March). Assessing the legality of data-localization requirements: Before the tribunals or at the negotiating table? *Columbia FDI Perspectives, No. 254.* Columbia Center on Sustainable Investment. https://ccsi.columbia.edu/content/columbia-fdi-perspectives

Dimitropoulos, G. (2025). Investment law and the digital economy. *Journal of International Dispute Settlement, 16*(1), 1–20. https://doi.org/10.1093/jids/idaf020

European Commission. (2024, July 1). *EU–Japan cross-border data flows deal enters into force* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3456

European Parliament. (2025, October 6). *Promoting and protecting digital sovereignty in the EU* [Debate].

Hepburn, J. (2017). Don't fence me in: Reforming trade and investment law to better facilitate cross-border data transfer. *Yale Journal of Law & Technology, 19*(1), 182–240.

Khan, A. N., Munir, B., & Ahmed, N. (2020). Critical analysis of bilateral investment treaties in Pakistan. *Journal of Research Society of Pakistan, 57*(3), 163–169.

Khan, A. N., Munir, B., & Jawwad, R. (2020). Evolution of protectionist approach for investor-state settlement of investment disputes: A critical analysis. *Pakistan Social Sciences Review, 4*(1), 893–906.

Kuner, C. (2013). *The regulation of transborder data flows under data protection and privacy law: Past, present and future* (OECD Digital Economy Papers No. 187). OECD Publishing. https://doi.org/10.1787/5k4c0mh3lq7j-en

Law Commission of England and Wales. (2023). *Digital assets: Final report.* London: Law Commission. https://www.lawcom.gov.uk/project/digital-assets/

Microsoft Corp. v. India, ITA No. 5844/2015 (Income Tax Appellate Tribunal, Dec. 2, 2019).

Munir, B. (2025). *Artificial intelligence for lawyers: Navigating novel methods and practices for the future of law.* Lahore: Punjab Law Book House.

OECD. (2019). *Going digital: Shaping policies, improving lives.* OECD Publishing. https://doi.org/10.1787/9789264312012-en

OECD. (2020). *Data localisation trends and challenges: Considerations for the review of the privacy guidelines* (A. Clement, Ed.; OECD Digital Economy Papers No. 290). OECD Publishing. https://doi.org/10.1787/3a5b703c-en

OECD. (2025). *UK interest in the Digital Economy Partnership Agreement (DEPA): DEPA joint statement (Final embargo).* OECD Digital Trade Forum.

Polanco, R. (2023). The impact of digitalization on international investment law: Are investment treaties analogue or digital? *German Law Journal, 24*(3), 574–596. https://doi.org/10.1017/glj.2023.45

Ramesh, V. (2018, October 8). Data protection principles around the world: Do they violate international investment law? *Völkerrechtsblog*. https://voelkerrechtsblog.org/data-protection-principles-around-the-world-do-they-violate-international-investment-law/

Raza, A., Munir, B., Ali, G., Othi, M. A., & Hussain, R. A. (2024). Balancing privacy and technological advancement in AI: A comprehensive analysis of the US perspective. *[Unpublished manuscript].*

Rudolf, P. D., & Schreuer, C. (2012). *Principles of international investment law* (2nd ed.). Oxford University Press.

Svantesson, D. (2019). *Internet & Jurisdiction global status report*. Internet & Jurisdiction Policy Network.

UK Government, Department for Business and Trade. (2024). *Smart data roadmap 2024–2025: The action the government is taking in 2024 to 2025* [Policy paper]. GOV.UK. https://www.gov.uk/government/publications/smart-data-roadmap-2024-to-2025

UNCTAD. (2021). *World investment report 2021: Investing in sustainable recovery*. United Nations. https://unctad.org/webflyer/world-investment-report-2021

UNCTAD. (n.d.). *IIA Navigator* (online database listing BIT exceptions). UNCTAD. Retrieved December 30, 2025, from https://investmentpolicy.unctad.org/international-investment-agreements

United Kingdom. (2025). *Property (Digital Assets etc) Act 2025*. London: The Stationery Office. https://www.legislation.gov.uk/ukpga/2025/29/enacted

Voss, G. (2020). Cross-border data flows, the GDPR, and data governance. *Washington International Law Journal, 29*(3), 485–520.

Wyman, O. (2021). *European digital sovereignty*. Oliver Wyman.

Zhang, Q., & Mitchell, A. (2022). Data localization and the national treatment obligation in international investment treaties. *World Trade Review, 21*(4), 391–403. https://doi.org/10.1017/S1474745622000213

IEER
Institute for Excellence in Education & Research