

УДК: [342.738.037:004.6]:351.86
[342.738.037:004.6]:[341:339]

**DATA LOCALISATION AND INTERNATIONAL ECONOMIC LAW:
RECONCILING DIGITAL SOVEREIGNTY WITH TRADE AND
INVESTMENT DISCIPLINES**

Pooja DAMODARAN

Vice President Legal, Siechem Technologies Pvt Ltd

PhD candidate, Mykolas Romeris University

e-mail: pooja@siechem.com; podamodaran@stud.mruni.eu

ORCID ID: 0009-0009-3990-6559

Abstract

This article examines whether state measures requiring data localisation, restricted transfer and increased regulatory control of platform generated data can be reconciled with international economic law (IEL). The central question is whether data localisation measures, justified on cybersecurity and sovereignty grounds, can satisfy the disciplines of market access, national treatment, and General Agreement on Trade in Services (GATS) Article XIV necessity test, and investment protection standards. While data localisation and cybersecurity policies reflect states' pursuit of digital sovereignty, they may simultaneously restrict cross border digital services, increase compliance costs for foreign platforms and affect digital investors. Using a doctrinal and comparative approach, the article analyses GATS Articles XVI, XVII and XIV, selected digital trade provisions in the United States-Mexico-Canada Agreement (USMCA) and Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), and investment law principles relating to fair and equitable treatment, indirect expropriation and police powers. China's Cybersecurity

Law is used as the main example. The article argues that IEL permits legitimate regulation of platform data, but only where such regulation is transparent, non-discriminatory, proportionate and not a disguised restriction on trade or investment.

Keywords: *Data Localisation, Digital Sovereignty, International Economic Law, Digital Trade, Investment Law*

1. Introduction

Technology has completely revolutionised the manner in which companies, particularly multinational companies working in the technology sector, manage their data collection, storage, and processing operations (Aaronson, 2018; United Nations Conference on Trade and Development [UNCTAD], 2021). With the continuous increase in digital footprint, governments around the world are focusing on the safeguarding of their national interests, the privacy of their citizens, and the control they can exercise over data generated within their territory (Chander & Lê, 2015; Sargsyan, 2016; R. D. Taylor, 2020). In addition, governments have begun to establish legislation mandating the localisation of data, meaning data cannot cross borders and must remain in its country of origin. However, such legislation does not develop in isolation but rather stand against established international practices (Burri, 2017; General Agreement on Trade in Services [GATS], 1994, arts. XVI–XVII; Mitchell & Hepburn, 2017).

As the global economy is digitising, several social media platforms have turned into opportunities for economic growth, political and cultural exchange (UNCTAD, 2021). Platforms like Meta's Facebook, TikTok, and X collect and store large amounts of user data to analyse and utilise them (Meta Platforms, Inc., n.d.; R. D. Taylor, 2020; TikTok, n.d.; X Corp., n.d.). These user data are beyond just numerical values; they are today the powerful tool that can influence individual and collective behaviour. Governments understand the value that social media has and its capacity to change, modify, or alter public behaviour or even serve interest of the nation (Chander & Lê, 2015; R. D. Taylor, 2020; UNCTAD, 2021).

In accordance with this, nations and their governments are issuing new policies that go to the extent of restricting, regulating or even banning certain digital platforms (Chander & Lê, 2015; R. D. Taylor, 2020). Other governments have made data localisation mandatory, where companies are required to comply with new regulatory controls over their digital assets and infrastructure. The concept of data localisation holds that information created within the borders of a particular nation should remain within its borders (Cohen et al., 2017; R. D.

Taylor, 2020). This is to help increase the government’s control over the flow of data and ensure its access to business operations’ data to protect the interests of the nation (Cohen et al., 2017).

These developments indicate a larger change in the manner in which the digital economy is regulated. Data localisation is no longer only a domestic regulatory issue. It also affects international trade and investment law because it may restrict cross border supply of services, change conditions of competition for foreign digital platforms, and impose additional obligations on foreign investors operating in the host state (Burri, 2017; Chander, 2020; GATS, 1994, arts. XVI–XVII; Mitchell & Hepburn, 2017).

This article asks whether measures requiring local storage, restricted transfer or increased regulatory control of platform generated data can be justified under IEL. The main focus is on GATS Articles XVI, XVII and XIV, selected digital trade provisions in USMCA and CPTPP, and investment law principles relating to fair and equitable treatment, indirect expropriation and police powers. The article adopts a doctrinal and comparative legal method by examining treaty provisions, case law and selected regulatory models, particularly China, the European Union and India. Cybersecurity is discussed only to the extent that it is used by states as a justification for data localisation.

2. Cybersecurity Threats and Data Localisation as a Regulatory Response

The field of cybersecurity is developing at an alarming rate in tandem with technology. As a result, the threats that both governments and citizens must contend with are becoming more varied. Cyberattacks can be carried out by state-sponsored groups, organised crime groups, or even lone hackers. Attacks can frequently be as straightforward as a typical phishing scam. Attacks, however, can occasionally become sophisticated, targeting infrastructure and potentially jeopardising national security. With threats constantly shifting and growing, states need to implement strong legal and regulatory systems along with active cybersecurity strategies to defend both public and private interests online (Kadena & Gupi, 2021). For the purpose of this article, however, cybersecurity threats are relevant only to the extent that they are used by states as legal and policy justifications for data localisation.

Cyberattacks, data breaches, cyber espionage and disruption of digital infrastructure may create genuine public risks. However, the existence of such risks does not automatically justify every localisation measure under IEL (GATS, 1994, art. XIV; World Trade Organization Appellate Body, 2005, 2016). A state must still show that measure is connected to the stated objective, that it

contributes to cybersecurity or public order, and that it does not operate as a disguised restriction on trade or investment.

2.1. Nature and Impact of Cybersecurity Threats

The impact of cyber-attacks is extensive and often serious. The consequences span financial, operational, and national security areas. For private entities, including investors, companies, and financial institutions, cyber incidents can cause major financial losses. They may also face regulatory fines for not following data protection and cybersecurity rules, as well as the risk of legal liability. Furthermore, these attacks can seriously harm their reputation, weakening stakeholder trust and reducing market value. Additionally, cyber-attacks may lead to unauthorized access, changes, or destruction of crucial data. This can disrupt business operations and long-term planning (Kadena & Gupi, 2021). Data localisation is a key measure adopted by the governments to safeguard and improve security and protection of data. The main arguments behind data localisation are, firstly to enhance the security by localising the data within the national borders, which way countries can control and protect personal sensitive data. Secondly, the governments believe the turnaround time for cyber threats would be much higher due to the proximity and convenient access of the processing facilities and finally; by introducing data localisation, governments invariably impose cyber security thresholds on the investors and ensure adherence to such standards (Cory & Dascoli, 2021; R. D. Taylor, 2020). However, such localisation measures may also create economic and legal burdens where they restrict cross border digital services or impose additional infrastructure costs on foreign suppliers (Bauer et al., 2014; Cory & Dascoli, 2021; Mitchell & Hepburn, 2017).

2.1.1. The case for data localisation as a cybersecurity measure

Data localisation is one of the main regulatory responses adopted by states to address cybersecurity, privacy and sovereignty concerns. It gives governments greater control over data generated within their territory and allows them to impose domestic compliance standards on foreign and domestic entities. Many countries have therefore adopted laws regulating how data is stored, processed and transferred across borders. These frameworks often include restrictions on cross-border data flows, mandatory data storage requirements for specific sectors such as finance, healthcare, or defence, and penalties for non-compliance. Initially, some of the world's most populous and digitally active countries took the lead in implementing strict data localisation measures. Notably, the European Union did this through the General Data Protection Regulation (GDPR), India through its Digital Personal Data Protection Act and proposed data

localisation clauses, and China via its Cybersecurity Law and Data Security Law, which impose strict controls on the export of data collected within its borders (Cybersecurity Law of the People’s Republic of China, 2017, art. 37; Data Security Law of the People’s Republic of China, 2021; Digital Personal Data Protection Act, 2023; Regulation (EU) 2016/679, 2016, arts. 44–49; Reserve Bank of India, 2018; R. D. Taylor, 2020).

However, now the effort has doubled, at least 62 countries as of 2021 have integrated data localisation and other relevant restrictions into their regulatory systems (Cory & Dascoli, 2021). There are two kinds of ways data localisation seems to have an effect, the first method being the “*hard*” data localisation or the *de facto* method, where the government has imposed complete restriction or prohibition of data to other countries and the second being “softer” or the *de jure* method, where data transfer remains permissible and legal, as long as a copy or mirrored data is stored in the country where it originated or generated (Cory & Dascoli, 2021; R. D. Taylor, 2020). This distinction is important because strict localisation has stronger consequences for trade in services and foreign digital investors.

For instance, legislations in Russia and China follow the “*hard*” data localisation method (Cybersecurity Law of the People’s Republic of China, 2017, art. 37; Federal Law No. 242-FZ, 2014; R. D. Taylor, 2020), where they restrict transfer of data generated within the territories. The China Cybersecurity law (Cybersecurity Law of the People’s Republic of China, 2017, art. 37; Qi et al., 2018) allows for certain data to be strictly stored domestically, where this also limits data transfer across border and protects national security. On the other hand, the “*soft*” data localisation is followed by countries such as India and Brazil (Digital Personal Data Protection Act, 2023; Lei Geral de Proteção de Dados Pessoais, 2018, arts. 33–36; Reserve Bank of India, 2018). The Reserve Bank of India (RBI) has mandated that all citizen data related payments ought to be stored within the country, though data transfers are allowed cross-borders, while also maintaining a copy locally, as for Brazil, the General Data Protection Law (LGPD) does not strictly impose on data localisation, however, require for certain threshold to be met while transferring data generated locally for overseas purposes (Digital Personal Data Protection Act, 2023; Lei Geral de Proteção de Dados Pessoais, 2018, arts. 33–36; Reserve Bank of India, 2018).

2.1.2. Data localisation impact on economic growth and other trade related activities:

While the states are imposing localisation strategy to tighten any concerns regarding cyber security, privacy and national sovereignty, there are also negative impacts on the economic and trade related activities which heavily rely on data transfers. Studies published on data localisation establish that the

strict data localisation regulations limit market access for foreign investors in states (Bauer et al., 2014; Cory & Dascoli, 2021). The business sectors reliant on free flow of data are hampered and restricted. Furthermore, critics argue that while data localisation may provide short-term control and a sense of security, it can isolate domestic markets, hinder technological progress, and provoke backlash from trade partners (Chander, 2020; Cory & Dascoli, 2021; Mitchell & Hepburn, 2017). This situation affects global digital trade negotiations. Balancing national interests with global economic integration is a complex challenge. Policymakers are increasingly required to create localisation laws that protect national data while promoting innovation and cross-border commerce.

In developing economies, data transfer and data sharing are primary source of economic growth, in Indonesia, it is estimated that due to data localisation policies, the country's economy will be down by 0.7% under an economy-wide localisation scenario, while investment losses under currently proposed measures are estimated at 2.3% (Bauer et al., 2014). The Japanese government having noted the impact of the strict regulatory regime for cross-border data transfer, has introduced the "Data Free Flow with Trust" (Arasasingham & Goodman, 2023) regulatory concept to encourage states to loosen the leash on data transfer and data localisation regimes.

Cybersecurity frameworks like Network and Information Security Directive (NIS2) and Digital Operational Resilience Act (DORA) were developed to strengthen EU privacy and security concerns (Directive (EU) 2022/2555, 2022; Espinoza et al., 2023; Regulation (EU) 2022/2554, 2022). NIS 2 is a legal directive which is required to be adopted by the host state (e.g. Germany has adopted the NIS2 Implementation Act – NIS2UmsCG) specifically focused on cybersecurity mechanism. Also, the DORA legislation is focused on risk management and reporting.

However, there is serious economic growth harms in data localisation including potential cybersecurity concerns. For instance, concentration of data within a specific location or a geographic area could potentially threat the entire volume of data to a phishing or malware attack (Baker et al., 2011; R. D. Taylor, 2020). Further, data localisation is also an inconvenience to multinational foreign investors as the access to these data are complex and more entry points for cyber hackers or criminals to use the data (Cory & Dascoli, 2021; R. D. Taylor, 2020). Also, as states are not unanimously adopting a common regulatory checks and balance system to manage data, the fragmentation of each host states' independent policies to manage cybersecurity strategy make it harder for global compliance and standards.

The traditional IEL frameworks were not designed to regulate data flows or platform related data inventory and address risks such as cyber-security, privacy and other data concerns. As a result, data localisation works as a mechanism and regime undertaken by States to ensure protection under data sovereignty, trade barriers and mitigating doctrinal boundaries between

legitimate expectations and digital protection (Burri, 2017; Mitchell & Hepburn, 2017; UNCTAD, 2021).

3. Comparative Regulatory Models of Data Localisation

Jurisdiction	Regulatory Approach	IEL relevance
China	Hard localisation and transfer review for critical information infrastructure, personal information and important data under the Cybersecurity Law (2017), Data Security Law (2021) and Personal Information Protection Law (2021) (Cybersecurity Law of the People’s Republic of China, 2017, art. 37; Data Security Law of the People’s Republic of China, 2021; Personal Information Protection Law of the People’s Republic of China, 2021)	Raises possible GATS Articles XVI and XVII concerns, and requires examination under the Article XIV necessity test and chapeau
EU	GDPR based transfer restriction model through adequacy decisions, appropriate safeguards and derogations, without imposing a general localisation requirement (Regulation (EU) 2016/679, 2016, arts. 44–49)	May indirectly affect cross-border digital services supplied by non-EU providers, primarily justified on privacy and fundamental rights grounds
India	Mixed model combining general transfer control under the Digital Personal Data Protection Act (2023) with sector specific localisation, particularly for payment data (Digital Personal Data Protection Act, 2023; Reserve Bank of India, 2018)	Raises concerns of regulatory uncertainty and compliance burden for foreign digital service suppliers.

The comparison above shows that data localisation practices are becoming increasingly common, but they do not operate in the same manner across jurisdictions (Cory & Dascoli, 2021; R. D. Taylor, 2020). Some states impose strict domestic storage requirements that limit or prohibit cross-border transfer altogether, while others regulate transfer through adequacy requirements,

safeguards or sector specific rules that permit movement of data subject to conditions (Cybersecurity Law of the People's Republic of China, 2017, art. 37; Data Security Law of the People's Republic of China, 2021; Personal Information Protection Law of the People's Republic of China, 2021; Regulation (EU) 2016/679, 2016, arts. 44–49; R. D. Taylor, 2020). From the perspective of international economic law, this distinction is important. A hard localisation rule that prevents cross-border supply of digital services entirely may raise stronger market access and national treatment concerns under GATS Articles XVI and XVII (Burri, 2017; GATS, 1994, arts. XVI–XVII; Mitchell & Hepburn, 2017) than a transfer safeguard model that conditions movement on compliance with protective standards. Similarly, the justification available to a state under GATS Article XIV will depend on the design of the specific measure and the evidence it can produce in support of the stated regulatory objective (GATS, 1994, art. XIV; World Trade Organization Appellate Body, 2005, 2016). The legality of any localisation measure therefore cannot be assessed in the abstract. It must be examined by reference to its design, the service sector affected, the commitments undertaken by the state, and the justification relied upon. The sections that follow carry out this analysis in relation to the principal legal frameworks applicable to data localisation under international economic law.

4. Data Localisation and International Economic Law

Data localisation requires data to be stored, processed, accessed or transferred subject to territorial conditions (Cohen et al., 2017; R. D. Taylor, 2020). Such measures pose a significant challenge to the basic principles of international economic law (Burri, 2017; Chander, 2020; GATS, 1994, arts. XVI–XVII; Mitchell & Hepburn, 2017). Agreements such as GATS, bilateral investment treaties, USMCA and CPTPP are based on market access, non-discrimination and cross border trade in services (Comprehensive and Progressive Agreement for Trans-Pacific Partnership [CPTPP], 2018, ch. 14; Dolzer & Schreuer, 2012; GATS, 1994, arts. XVI–XVII; United States–Mexico–Canada Agreement [USMCA], 2018, ch. 19). Data localisation rules may therefore work as regulatory barriers, even where they are presented as cybersecurity, privacy or sovereignty measures (Burri, 2017; Chander, 2020; Cory & Dascoli, 2021; Mitchell & Hepburn, 2017).

4.1. GATS Analysis: Market Access, National Treatment and Article XIV

Trade law limits data localisation measures through the GATS where a WTO Member has undertaken specific commitments in the relevant service

sector (GATS, 1994, art. XX; World Trade Organization, n.d.). Articles XVI and XVII become important in this regard. Article XVI deals with market access, while Article XVII deals with national treatment. Therefore, a data localisation measure may raise a GATS issue if it prevents cross border supply of digital services, requires local infrastructure as a condition of business, or changes the conditions of competition against foreign service suppliers.

The first step is to identify the relevant service sector. This is important because digital platform services do not fall under one single agreed classification (Burri, 2017; World Trade Organization, 1991). The analysis would require a preliminary determination of which GATS sector covers the relevant platform activity, as China’s specific commitments vary considerably between computer services, telecommunications and audio-visual categories (World Trade Organization, 2002). Once the sector and commitment are identified, the next question is whether the measure restricts market access under Article XVI or affects national treatment under Article XVII.

Even if a breach is found, the state may rely on GATS Article XIV. However, Article XIV does not give a general permission to restrict data flows (GATS, 1994, art. XIV; World Trade Organization Appellate Body, 2005, 2016). The state must show that the measure falls within a recognised public policy ground, such as public order, privacy or protection of confidential information (GATS, 1994, art. XIV). It must also show that the measure is necessary and that there are no reasonably available less trade restrictive alternatives (World Trade Organization Appellate Body, 2005, 2016). The measure must also satisfy the chapeau of Article XIV, meaning that it should not be applied in an arbitrary or discriminatory manner or as a disguised restriction on trade. US Gambling and Argentina Financial Services are useful authorities for this structured approach because they show that exceptions must be supported by evidence and cannot be accepted only on the basis of a general policy claim (World Trade Organization Appellate Body, 2005, 2016).

4.2. Application of GATS Article XIV to China’s Cybersecurity Law

China’s Cybersecurity Law provides the clearest example for applying this test (Cybersecurity Law of the People’s Republic of China, 2017, art. 37; Qi et al., 2018). Its localisation and transfer review requirements may be defended as cybersecurity and national security measures (Cybersecurity Law of the People’s Republic of China, 2017, art. 37; Data Security Law of the People’s Republic of China, 2021; Personal Information Protection Law of the People’s Republic of China, 2021). However, under GATS Article XIV, a WTO panel would not stop at the stated objective of the law (World Trade Organization Appellate Body, 2005, 2016). It would examine whether the measure actually contributes to cybersecurity, whether the measure is necessary, and whether less

trade restrictive alternatives are reasonably available. Such alternatives may include encryption, targeted security audits, certification, contractual safeguards, adequacy style mechanisms or narrower sector specific controls (Chander, 2020; Regulation (EU) 2016/679, 2016, arts. 44–49; R. D. Taylor, 2020).

Therefore, a broad localisation duty covering ordinary commercial platform data would be harder to justify than a narrow rule limited to genuinely sensitive data or critical infrastructure (Chander, 2020; GATS, 1994, art. XIV; World Trade Organization Appellate Body, 2005, 2016). China may have stronger justification where the measure concerns critical information infrastructure or important data, but the justification becomes weaker if the same restrictions apply broadly to ordinary business data without clear evidence of risk. This shows the main tension under international economic law: digital sovereignty and cybersecurity are legitimate concerns, but they must still satisfy the legal tests of necessity, non-discrimination and proportionality.

4.3. Digital Trade Agreements: USMCA and CPTPP

Recent digital trade agreements address data localisation more directly than the GATS. USMCA Article 19.11 protects cross border transfer of information by electronic means for business purposes, while Article 19.12 restricts parties from requiring the use or location of computing facilities in their territory as a condition for conducting business. (USMCA, 2018, arts. 19.11–19.12) The CPTPP (CPTPP, 2018, arts. 14.11, 14.13) adopts a similar approach in its electronic commerce chapter. These agreements do not completely take away the regulatory space of states. They allow legitimate public policy measures where such measures are not arbitrary, discriminatory or disguised restrictions on trade (CPTPP, 2018, arts. 14.11, 14.13; USMCA, 2018, arts. 19.11–19.12). This shows a balanced model where cross border data flows remain important for digital trade, but cybersecurity, privacy and public policy also remain valid regulatory concerns.

4.4. Data Localisation under Investment Law

For investment law, foreign digital platforms may bring claims where localisation measures interfere with protected investments, impose additional infrastructure costs, or substantially affect the use, value or control of the investment (CPTPP, 2018, ch. 14; Dolzer & Schreuer, 2012; UNCTAD, 2012; USMCA, 2018, ch. 19). The most relevant claims would be based on fair and equitable treatment and indirect expropriation. However, not every regulatory change will amount to a treaty breach. A localisation measure adopted in good faith for cybersecurity, privacy or public order may fall within the state's police powers, particularly where it is transparent, non-discriminatory and

proportionate. The difficulty arises where the measure is vague, sudden, discriminatory, or framed as cybersecurity regulation while actually protecting domestic firms from foreign competition.

The investment arbitration cases that are most relevant to this analysis each address a different dimension of the problem. In *Tecmed v Mexico* (Técnicas Medioambientales Tecmed, S.A. v. United Mexican States, 2003, para. 154), the tribunal found that a regulatory decision which frustrated the investor's legitimate expectations by departing abruptly from the conditions under which the investment was originally made could constitute a violation of the fair and equitable treatment standard. Applied to data localisation, this is significant because a foreign digital platform that structured its operations in a particular territory on the basis of an existing regulatory environment may have a legitimate expectation that fundamental rules governing data storage and transfer will not change without reasonable notice, transparency, or justification. Where a state imposes sudden or unpredictable localisation requirements without clear standards or a transitional period, the reasoning in *Tecmed* becomes directly relevant to whether an FET claim could succeed. *Pope & Talbot v Canada* (Pope & Talbot Inc. v. Government of Canada, 2000) approaches the same problem from the opposite direction. The tribunal there recognised that regulatory measures of general application, enacted in good faith and without discriminating against the foreign investor specifically, will not ordinarily amount to indirect expropriation even where they impose compliance costs or affect profitability. This is important in the data localisation context because it confirms that a foreign digital platform cannot simply point to increased infrastructure costs or operational disruption as sufficient grounds for an expropriation claim. The measure must go considerably further and substantially deprive the investor of the use, value or control of its investment before expropriation becomes arguable.

Further, in the case of *Philip Morris v Uruguay* (Philip Morris Brands Sàrl v. Oriental Republic of Uruguay, 2016, paras. 418–422) reinforces this by confirming that where a state adopts a measure in bona fide pursuit of a legitimate public interest, such as public health in that case, or by analogy cybersecurity and public order in the data localisation context, and does so in a non-discriminatory and proportionate manner, the measure will fall within the state's police powers and will not give rise to compensable liability under investment law. The difficulty, however, is illustrated by *Cargill v Mexico* (Cargill, Inc. v. United Mexican States, 2009, paras. 361–365), where the tribunal found that measures adopted ostensibly in a regulatory capacity could still breach investment obligations where they imposed burdens on the foreign investor that were not justified by the stated objective and operated in a discriminatory manner. In the data localisation context, this means that a state cannot rely on a general invocation of cybersecurity or digital sovereignty to insulate a localisation measure from investment law scrutiny. If the measure is applied selectively

against foreign platforms, imposes requirements that exceed what the cybersecurity objective actually demands, or operates to benefit domestic competitors, it may fall outside the protection of the police powers doctrine and attract liability under the FET standard or the indirect expropriation provisions of the applicable treaty. Together, these cases establish that the central investment law question in any data localisation dispute is not simply whether the state had a regulatory purpose, but whether the measure was designed and applied in a manner that is genuinely connected to that purpose, proportionate in its burden, and non-discriminatory in its operation.

4.5. Cybersecurity Risks of Localisation and Comparative State Approaches

Although data localisation is intended to be seen as a cybersecurity tactic, it has drawbacks of its own (Chander, 2020; R. D. Taylor, 2020). When it comes to cyberattacks, the concentration of data within a single geographic jurisdiction makes an attractive target. The difficulties are further compounded by inadequate infrastructure and inconsistent national standards. When data is concentrated in one area, it creates what is known as "a single point of failure," which gives an attacker unrestricted access to massive amounts of private information (Baker et al., 2011; R. D. Taylor, 2020).

Investors have some issues as a result of the aforementioned modifications. Due to the increased cost of ensuring compliance, the first issue is related to compliance. Second, it becomes more difficult to obtain information and deal with the potential for liability. Lastly, the processes of risk management and due diligence are complicated by the non-standardization process (Bauer et al., 2014; Cory & Dascoli, 2021; Mitchell & Hepburn, 2017).

Data localisation is a topic that many jurisdictions address, and it involves not just regulations but also ideological and moral disparities. (Meltzer, 2013) In order to promote free data flows, the US crafts trade rules that, if feasible, reject localisation requirements (Office of the United States Trade Representative, n.d.; USMCA, 2018, arts. 19.11–19.12). However, the GDPR, which limits data transfers to nations unless they ensure a high level of protection, is the foundation of the European Union's privacy-first strategy. Although GDPR (Regulation (EU) 2016/679, 2016, arts. 44–49), does not formally require data to remain local, in reality it restricts communication with nations without an adequacy ruling, which is a barrier motivated by basic rights (Data Protection Commissioner v. Facebook Ireland Ltd, 2020; Regulation (EU) 2016/679, 2016, arts. 44–49).

The People's Republic of China represents a highly interventionist model. Its Cybersecurity Law (2017), Data Security Law (2021), and Personal Information Protection Law (2021) (Cybersecurity Law of the People's Republic of China, 2017, art. 37; Data Security Law of the People's Republic of China, 2021; Personal Information Protection Law of the People's Republic of China,

2021) require that certain types of crucial data stay within the country, with strict security checks before anything crosses the border. The European Union follows a different model. The GDPR does not impose general localisation, but restricts transfers to jurisdictions that do not ensure adequate protection. India reflects an intermediate position, combining general transfer regulation under the Digital Personal Data Protection Act, 2023 (Digital Personal Data Protection Act, 2023; Reserve Bank of India, 2018) with sector specific localisation obligations, particularly in payment data. These differences show that digital sovereignty does not take a single form. For international economic law, the relevant question is whether each model is designed and applied in a manner consistent with market access, non-discrimination, necessity and proportionality (Burri, 2017; GATS, 1994, arts. XVI–XVII; Mitchell & Hepburn, 2017).

4.6. Rethinking International Economic Law in the Digital Age

The analysis in the preceding sections makes it clear that the existing framework of international economic law was not originally designed to address platform generated data, cross-border digital services, or the kind of sovereignty concerns that data localisation now raises (UNCTAD, 2021). GATS was negotiated before digital platforms and cross-border data flows became central regulatory concerns (Burri, 2017; UNCTAD, 2021; World Trade Organization, 1998). Similarly, bilateral investment treaties developed mainly around traditional commercial enterprises, physical assets and conventional forms of foreign investment (Dolzer & Schreuer, 2012; UNCTAD, 2011). When a government today requires a social media company to store user data domestically, or subjects outbound data transfers to national security review, the legal tools available under GATS Articles XVI, XVII and XIV, and under investment law standards such as fair and equitable treatment and indirect expropriation, can be applied, but not without difficulty.

This, however, does not imply that international economic law is incapable of responding to such regulatory challenges. As the preceding discussion shows, the necessity test, proportionality reasoning in the police powers doctrine, and the chapeau requirements under Article XIV provide a workable basis for distinguishing legitimate regulation from disguised protectionism (GATS, 1994, art. XIV; *Philip Morris Brands Sàrl v. Oriental Republic of Uruguay*, 2016; *Pope & Talbot Inc. v. Government of Canada*, 2001; World Trade Organization Appellate Body, 2005, 2016). However, applying these tests to platform data requires international economic law to take seriously something it has not traditionally confronted in this form, namely that data is not simply a service input (L. Taylor, 2017; R. D. Taylor, 2020; UNCTAD, 2021). Controlling where it is stored can mean something very different from regulating how a service is delivered.

For social media companies and other digital platforms, cross-border data flows are not merely incidental to business operations. They are often central to content moderation, advertising systems, cybersecurity monitoring, user authentication and overall platform management (Meta Platforms, Inc., n.d.; TikTok, n.d.; UNCTAD, 2021; X Corp., n.d.). A localisation requirement affecting these functions does not operate like an ordinary tariff or quota. It reaches into the operating architecture of the platform itself and can affect both the trade and investment dimensions of the company's presence in a given territory. This is why the legal analysis of data localisation cannot be reduced to a single question of market access or investor protection. It requires attention to both, and any future development of international economic law in this area will need to reflect that reality.

Recognising this does not mean that states should be free from international economic law disciplines whenever they invoke cybersecurity or digital sovereignty. The necessity test under GATS Article XIV already draws a distinction between genuine public policy justifications and regulatory measures that use the language of security to shelter domestic firms from foreign competition (GATS, 1994, art. XIV; World Trade Organization Appellate Body, 2005, 2016). A narrow localisation rule covering only genuinely critical infrastructure data, or data with demonstrable national security significance, is in a much stronger legal position than a broad requirement covering all personal data collected on any platform operating within the territory. In the latter case, the state would face a considerably higher evidentiary burden to show why territorial storage specifically, rather than encryption, targeted audits, certification or contractual safeguards, is necessary to achieve the stated objective (Burri, 2017; GATS, 1994, arts. XVI–XVII; Mitchell & Hepburn, 2017; R. D. Taylor, 2020). As the discussion of China's Cybersecurity Law above illustrates, the breadth of the measure is directly relevant to how difficult it becomes to justify under the necessity and chapeau requirements of Article XIV.

Data justice is also worth considering in this context, though not as a standalone exception to trade or investment disciplines. The point is a limited one. Platform data is not the same as other commercial inputs because it carries personal information, behavioural patterns, political expression and content generated by individuals and communities (Chander & Lê, 2015). When states regulate this kind of data, they are not always acting as protectionists. Sometimes they are responding to legitimate concerns about privacy, representation and accountability of large digital platforms. International economic law should be capable of recognising this distinction. The GDPR adequacy framework, for instance, shows that rights-based data governance and cross-border trade can coexist in practice, even if imperfectly (Chander, 2020; Regulation (EU) 2016/679, 2016, arts. 44–49). The challenge for international economic law is to absorb this kind of regulatory purpose without allowing it to become a blanket

justification for any restriction a state chooses to impose on foreign digital service providers.

The path forward is therefore a more disciplined and context sensitive application of the legal tools already available, rather than a wholesale redesign of international economic law institutions. Necessity, proportionality, non-discrimination and transparency are already present in the GATS framework and in investment treaty jurisprudence. What is needed alongside these is stronger international coordination, through adequacy arrangements, mutual recognition of cybersecurity standards, sector-specific transfer safeguards and narrowly tailored localisation requirements for genuinely sensitive data (Arasasingham & Goodman, 2023; CPTPP, 2018, arts. 14.11, 14.13; Regulation (EU) 2016/679, 2016, arts. 44–49; USMCA, 2018, arts. 19.11–19.12). This would allow states to pursue legitimate data governance objectives without unnecessarily fragmenting the digital trade environment or triggering avoidable trade disputes and investment treaty claims. Such an approach allows international economic law to respond to digital sovereignty concerns without abandoning its core commitments to market access, fair treatment and cross-border economic cooperation.

Conclusion

Data localisation has become one of the key ways through which states assert digital sovereignty over platform-generated data. Although such measures may be justified on grounds of cybersecurity, privacy, law enforcement and public order, they also affect cross-border digital services and the position of foreign investors in the host state. This creates a direct tension with international economic law, especially because the existing framework was not designed with platform data and digital services as central concerns.

This article has argued that data localisation is not inherently unlawful under international economic law. States retain the authority to regulate for legitimate public purposes, but such authority is not unlimited. Under GATS, localisation measures may raise market access and national treatment concerns where they restrict cross-border supply or alter conditions of competition. Such measures may still be justified under Article XIV, but only where they are necessary, proportionate, non-discriminatory and not applied as disguised restrictions on trade.

The investment law position is similarly balanced. Data localisation may affect the expectations, costs and business models of foreign digital platforms, but fair and equitable treatment and indirect expropriation standards do not protect investors from every regulatory change. A genuine, proportionate and non-discriminatory measure adopted for cybersecurity, privacy or public order

may fall within the state's police powers. However, vague, excessive, discriminatory or protectionist localisation measures may still attract liability.

The example of China's Cybersecurity Law reflects this difficulty. While localisation and transfer review may be justified for cybersecurity and national security, broad restrictions on ordinary commercial data flows become harder to reconcile with international economic law where they lack transparency, clear standards or a demonstrable connection to the stated risk. The same analytical framework applies, with varying intensity, to the EU's adequacy-based transfer model and India's mixed regulatory approach.

International economic law must therefore respond to the digital economy by applying its existing disciplines with greater sensitivity to how platform data functions. The better approach lies between unrestricted data liberalisation and absolute territorial control. States should pursue data governance through necessity, proportionality, transparency, non-discrimination and narrowly tailored localisation for genuinely sensitive data, while preserving the conditions necessary for cross-border digital trade and investment.

Acknowledgement

The author used the generative AI tool ChatGPT (OpenAI, GPT-5, 2025 version) only for limited editorial assistance in improving language clarity, paragraph flow and structural organisation in the abstract, introduction and background portions of the article. The legal analysis, case selection, citations, conclusions and final arguments were independently reviewed, verified and approved by the author, who assumes full responsibility for the manuscript.

References

- Aaronson, S. A. (2018). *Data is different: Why the world needs a new approach to governing cross-border data flows* (CIGI Paper No. 197). Centre for International Governance Innovation.
<https://www.cigionline.org/publications/data-different-why-world-needs-new-approach-governing-cross-border-data-flows/>
- Arasasingham, A., & Goodman, M. P. (2023, April 13). *Operationalizing data free flow with trust (DFFT)*. Center for Strategic and International Studies. <https://www.csis.org/analysis/operationalizing-data-free-flow-trust-dfft>

- Baker, W., Goudie, M., Hutton, A., Hylender, C. D., Niemantsverdriet, J., Novak, C., Ostertag, D., Porter, C., Rosen, M., Sartin, B., & Tippet, P. (2011). *2011 data breach investigations report*. Verizon RISK Team.
- Bauer, M., Lee-Makiyama, H., van der Marel, E., & Verschelde, B. (2014). *The costs of data localisation: Friendly fire on economic recovery* (ECIPE Occasional Paper No. 3/2014). European Centre for International Political Economy. <https://ecipe.org/publications/the-costs-of-data-localisation/>
- Burri, M. (2017). The governance of data and data flows in trade agreements: The pitfalls of legal adaptation. *UC Davis Law Review*, 51(1), 65–132.
- Cargill, Incorporated v. United Mexican States, ICSID Case No. ARB(AF)/05/2, Award (September 18, 2009).
- Chander, A. (2020). Is data localization a solution for Schrems II? *Journal of International Economic Law*, 23(3), 771-784. <https://doi.org/10.1093/jiel/jgaa024>
- Chander, A., & Lê, U. P. (2015). Data nationalism. *Emory Law Journal*, 64(3), 677–739.
- Cohen, B., Hall, B., & Wood, C. (2017). Data localization laws and their impact on privacy, data security and the global economy. *Antitrust*, 32(1), 107–114.
- Comprehensive and Progressive Agreement for Trans-Pacific Partnership*. (2018). <https://www.mfat.govt.nz/assets/Trade-agreements/CPTPP/Comprehensive-and-Progressive-Agreement-for-Trans-Pacific-Partnership-CPTPP-English.pdf>
- Cory, N., & Dascoli, L. (2021). *How barriers to cross-border data flows are spreading globally, what they cost, and how to address them*. Information Technology and Innovation Foundation. <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost-and-how-to-address-them/>
- Cybersecurity Law of the People's Republic of China*. (2017).
- Data Protection Commissioner v. Facebook Ireland Ltd and Maximilian Schrems*, Case C-311/18, ECLI:EU:C:2020:559 (2020).
- Data Security Law of the People's Republic of China*. (2021).
- Digital Personal Data Protection Act*, No. 22 of 2023, India Code (2023).
- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, 2022 O.J. (L 333) 80.
- Dolzer, R., & Schreuer, C. (2012). *Principles of international investment law* (2nd ed.). Oxford University Press.
- Espinoza, F., Maryska, M., Doucek, P., & Kovářová, M. (2023). DORA and NIS2 and their impact on database security. In *IDIMT 2023: New challenges for ICT and management-31st Interdisciplinary Information*

- Management Talks* (pp. 81–87). <https://doi.org/10.35011/IDIMT-2023-81>
- Federal Law No. 242-FZ of 21 July 2014 amending Federal Law No. 152-FZ on Personal Data* (Russia). (2014).
- General Agreement on Trade in Services*, April 15, 1994, 1869 U.N.T.S. 183.
- Kadena, E., & Gupi, M. (2021). Human factors in cybersecurity: Risks and impacts. *Security Science Journal*, 2(2), 51–64. <https://doi.org/10.37458/ssj.2.2.3>
- Lei Geral de Proteção de Dados Pessoais* [General Data Protection Law], Law No. 13,709/2018 (Brazil). (2018).
- Meltzer, J. P. (2013). *The internet, cross-border data flows and international trade* (Issues in Technology Innovation No. 22). Brookings Institution. <https://doi.org/10.2139/ssrn.2292477>
- Meta Platforms, Inc. (n.d.). *Privacy policy*. Retrieved July 16, 2026, from <https://www.facebook.com/privacy/policy/>
- Mitchell, A. D., & 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, 182–237.
- Office of the United States Trade Representative. (n.d.). *USMCA Chapter 19: Digital trade*. Retrieved July 16, 2026, from <https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf>
- Personal Information Protection Law of the People's Republic of China*. (2021).
- Philip Morris Brands Sàrl, Philip Morris Products S.A. and Abal Hermanos S.A. v. Oriental Republic of Uruguay*, ICSID Case No. ARB/10/7, Award (July 8, 2016).
- Pope & Talbot Inc. v. Government of Canada*, UNCITRAL, Award on the Merits, Phase 2 (June 26, 2000).
- Qi, A., Shao, G., & Zheng, W. (2018). Assessing China's cybersecurity law. *Computer Law & Security Review*, 34(6), 1342-1354. <https://doi.org/10.1016/j.clsr.2018.08.007>
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1.
- Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector, 2022 O.J. (L 333) 1.
- Reserve Bank of India. (2018, April 6). *Storage of payment system data* (Circular No. DPSS.CO.OD No. 2785/06.08.005/2017-18). <https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244>
- Sargsyan, T. (2016). Data localization and the role of infrastructure for surveillance, privacy, and security. *International Journal of Communication*, 10, 2214-2237.

- Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society*, 4(2), 1-14. <https://doi.org/10.1177/2053951717736335>
- Taylor, R. D. (2020). "Data localization": The internet in the balance. *Telecommunications Policy*, 44(8), Article 102003. <https://doi.org/10.1016/j.telpol.2020.102003>
- Técnicas Medioambientales Tecmed, S.A. v. United Mexican States*, ICSID Case No. ARB(AF)/00/2, Award (May 29, 2003).
- TikTok. (n.d.). *Privacy policy*. Retrieved July 16, 2026, from <https://www.tiktok.com/legal/page/row/privacy-policy/en>
- United Nations Conference on Trade and Development. (2011). *Scope and definition: UNCTAD series on issues in international investment agreements II*. United Nations.
- United Nations Conference on Trade and Development. (2012). *Expropriation: UNCTAD series on issues in international investment agreements II*. United Nations.
- United Nations Conference on Trade and Development. (2021). *Digital economy report 2021: Cross-border data flows and development-For whom the data flow*. United Nations. https://unctad.org/system/files/official-document/der2021_en.pdf
- United States–Mexico–Canada Agreement*. (2018). <https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf>
- World Trade Organization. (n.d.). *Schedules of specific commitments and lists of Article II exemptions*. Retrieved July 16, 2026, from https://www.wto.org/english/tratop_e/serv_e/serv_commitments_e.htm
- World Trade Organization. (1991, July 10). *Services sectoral classification list* (MTN.GNS/W/120).
- World Trade Organization. (1998, September 30). *Work programme on electronic commerce* (WT/L/274).
- World Trade Organization. (2002, February 14). *China-Schedule of specific commitments* (GATS/SC/135).
- World Trade Organization Appellate Body. (2005). *United States-Measures affecting the cross-border supply of gambling and betting services* (WT/DS285/AB/R).
- World Trade Organization Appellate Body. (2016). *Argentina-Measures relating to trade in goods and services* (WT/DS453/AB/R).
- X Corp. (n.d.). *Privacy policy*. Retrieved July 16, 2026, from <https://x.com/en/privacy>