國立臺灣大學法律學院法律學系

碩士論文

Department of Law

College of Law

National Taiwan University

Master Thesis

世界貿易組織規範資料在地儲存要求之芻議

Proposing the Regulation of Local Storage Requirements under the World Trade Organization

葉家瑄

Chia-Hsuan Yeh

指導教授：楊岳平 博士

Advisor: Yueh-Ping Yang, S.J.D.

中華民國 113 年 7 月

July 2024

doi:10.6342/NTU202402499

國立臺灣大學碩士學位論文
口試委員會審定書

世界貿易組織規範資料在地儲存要求之芻議

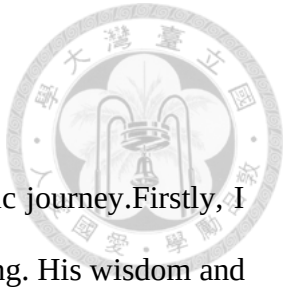
Proposing the Regulation of Local Storage Requirements under the World Trade Organization

本論文係葉家瑄君（學號:R10A21090）在國立臺灣大學法律學系完成之碩士學位論文，於民國113年7月26日承下列考試委員審查通過及口試及格，特此證明

指導教授：

口試委員：

doi:10.6342/NTU202402499



ACKNOWLEDGEMENTS

I am grateful to everyone who has supported me on my academic journey.Firstly, I would like to express my deepest thanks to my mentor, Professor Yang. His wisdom and attitude have been a source of inspiration throughout the completion of this thesis. I first met Professor Yang when I joined the NTU WTO representative team as a first-year graduate student, and since then, he has been a tremendous encouragement in many ways. He once told me, “When you are in your youth, you can also try to push yourself harder.” These words became the driving force behind my persistence in finishing this thesis.

Frankly speaking, I considered giving up several times during my academic pursuit, especially when I was exhausted after working during the daytime. However, upon completing this thesis, I did not dwell on the difficulties I once viewed as obstacles. Instead, what remains deeply ingrained in my mind is what I learned from Professor Yang and the research process.I would also like to extend my gratitude to Professor Tsai-yu Lin. During my first year as a graduate student, I took Professor Lin’s courses on WTO law and investment law, where I learned the fundamentals of English academic writing. Completing this thesis in English would not have been possible without the foundational skills I acquired from Professor Lin’s courses.Thanks to my parents and family. Without your love, I would not have had the courage to face the ups and downs of this journey. I am also grateful to my colleagues from the NTU WTO representative team. I will always cherish the time we spent together preparing for the J.H. Jackson Moot Court Competition. My thanks also go to my colleagues from the NTU International Law Program. Your support was invaluable in the successful publication of my thesis.

Finally, I would like to thank Alva for always being by my side whenever I needed support. Before pursuing my master’s degree at National Taiwan University, I was

doi:10.6342/NTU202402499

practicing law at a Taiwanese law firm. Returning to school was a significant and challenging commitment for me. While studying, I sometimes felt anxious and had second thoughts about my decision to pursue a master's degree, especially when I saw my former colleagues advancing in their careers. However, with the support of my professors, friends, and family, I was able to overcome these doubts and complete my academic journey.

doi:10.6342/NTU202402499

CHINESE ABSTRACT

於數位化時代下，資料的重要性逐漸被各國政府所重視，進而導致資料在地化法規之施行數量逐年攀升。目前資料在地化措施並無普遍性的定義，惟其通常泛指在特定的司法管轄區內規定數據的存儲、處理或轉移的法規、命令或行政要求。本論文聚焦於研究資料本地儲存規範對於貿易產生的負面影響，檢驗其與服務貿易總協定之間的相容性，並探討前述協定是否足以規範數據本地儲存規範對服務貿易衍生的負面貿易效應。

目前 WTO 電子商務聯合聲明倡議中，日本及美國皆曾相繼主張應明文禁止資料本地儲存規範，顯見既有的服務貿易總協定似仍不足因應資料本地儲存規範衍生的貿易負面效應。因此，本文亦一併審視各種區域貿易協定及數位經濟協議中存在的「計算設施位置」條款。「計算設施位置」條款廣泛性地禁止資料本地儲存規範作為締約國內進行商業活動的條件，此類條款之規範模式或許可成為日後國際經貿組織監管此類規範之參考依據。本論文的最終目標，旨在透過文獻分析及比較法學研究，向世界貿易組織提議一個規範模式，以此消弭資料本地儲存規範所生之貿易壁壘。

關鍵詞：資料在地化政策、資料本地儲存規範、服務貿易總協定、計算設施位置條款、數位經濟協議

doi:10.6342/NTU202402499

ENGLISH ABSTRACT

In today's digital era, data localisation policies have sparked debates regarding their impact on international trade and e-commerce. Data localisation is an ambiguous concept without a universal definition, which can broadly encompass laws, regulations, or administrative requirements mandating the storage, processing, or transfer of data within specific jurisdictions. This thesis particularly focuses on studying the trade implications of local storage requirements and examinines their compatibility with the General Agreement on Trade in Services (GATS).

Moreover, since a few WTO Members have advocated for the prohibition of local storage requirements under the Joint Statement Initiative, the adequacy of the existing GATS in addressing the trade impact of such requirements may be questioned from the perspectives of certain Members. Therefore, this thesis seeks to derive insights from the "location of computing facilities" clauses present in various Regional Trade Agreements and Digital Economic Agreements. These clauses typically forbid covered persons from using or locating computing facilities in that Party's territory as a condition for conducting business in that territory. This thesis aims to propose a potential regulatory framework for local storage requirements within the WTO's e-commerce context.

KEYWORDS: *Data localisation, Local Storage Requirements, GATS, Location of Computing Facilities, Digital Economic Agreements*

doi:10.6342/NTU202402499

TABLE OF CONTENTS

doi:10.6342/NTU202402499

doi:10.6342/NTU202402499

doi:10.6342/NTU202402499

doi:10.6342/NTU202402499

doi:10.6342/NTU202402499

doi:10.6342/NTU202402499

doi:10.6342/NTU202402499

doi:10.6342/NTU202402499

CHAPTER ONE INTRODUCTION

I. BACKGROUND TO THE RESEARCH

A. The Proliferation of Data Localisation Rules and Their Trade Impacts

Ever since the Internet was invented on January 1, 1983,[1] it has heralded a new chapter in the digital era. In this digital landscape, data has emerged as the new oil.[2] Data refers to facts and statistics collected together for reference or analysis.[3] Its utility spans enhancing decision-making processes, innovating new products and services, optimizing operational efficiency, personalizing customer experiences, and even serving as tradable commodities among businesses.[4]

Trade and production are increasingly reliant on the processing, storage, and transfer of data[5] The cross-border movement of data, or information, plays a pivotal role in the emergence of new and rapidly expanding goods and service supply models. Moreover, it underpins trade by facilitating the coordination of Global Value Chains (hereinafter "GVCs") and the implementation of more efficient trade facilitation mechanisms.[6]

Furthermore, data constitutes a vital asset for information and communication technology (hereinafter "ICT") companies to thrive and progress. For instance, data analytics which necessitate vast datasets hold a pivotal role in the operations of ICT

[1] Barry M. Leiner, et al., *A Brief History of the Internet*., 39 ACM SIGCOMM COMPUT. COMMUN. REV. 22, 29 (2009).
[2] David Parkins, *The World's Most Valuable Resource is No Longer Oil, but Data,* THE ECONOMIST (May. 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (last visited Apr. 10, 2024).
[3] WHAT IS DATA, https://dataschools.education/about-data-literacy/what-is-data/ (last visited Apr. 10, 2024).
[4] *Unleashing the Value of Data: Exploring Why Data is the New Gold*, SECURITY PRIVACY (Oct. 20, 2023), https://secureprivacy.ai/blog/significance-of-data-in-digital-era (last visited Apr. 10, 2024).
[5] JAVIER LÓPEZ-GONZÁLEZ & M. JOUANJEAN, OECD TRADE POLICY PAPERS NO.205 DIGITAL TRADE: DEVELOPING A FRAMEWORK FOR ANALYSIS 6.
[6] *Id*. at 4.

doi:10.6342/NTU202402499

firms.[7] According to Mathias Cormann, the Secretary-General of the Organization for Economic Cooperation and Development (hereinafter "OECD"), "the Information and Communication Technology sector is a major force behind global growth."[8]

In this digital era, data is increasingly being recognized as a valuable asset by governments, leading to the implementation of numerous data governance regulations aimed at controlling where data can be used, transferred, processed, collected, and stored across nations.[9] These measures are commonly known as the so-called "data localisation" policies.[10]

According to a 2021 report issued by the Information Technology & Innovation Foundation (hereinafter "ITIF report"), the number of data-localisation measures worldwide has more than doubled from 2017 to 2021.[11] The ITIF report constructed models utilizing a scale derived from OECD market regulation data. The analysis revealed that for every 1-point increment in a country's data restrictiveness, there is a corresponding 7 percent reduction in its gross trade output, a 2.9 percent decrease in productivity, and a 1.5 percent increase in downstream prices over a five-year period.[12] Consequently, data localisation measures invariably lead to adverse effects on trade.

The increasing prominence of data-driven innovation and digital-enabled trade underscores the growing significance of data in the global economy. In addition, the Secretary-General of the Digital Cooperation Organization expected that the digital

[7] NVIT, *Data Analytics in ICT*, LINKEDIN (May, 24, 2023), https://www.linkedin.com/pulse/data-analytics-ict-nvitech.
[8] *Growth of digital economy outperforms overall growth across OECD*, OECD (May 14, 2024), https://www.oecd.org/newsroom/growth-of-digital-economy-outperforms-overall-growth-across-oecd.htm.
[9] NIGEL CORY & LUKE DASCOLI, HOW BARRIERS TO CROSS-BORDER DATA FLOWS ARE SPREADING GLOBALLY, WHAT THEY COST, AND HOW TO ADDRESS THEM 1 (2021).
[10] *Id.*
[11] *Id.*
[12] *Id.*

doi:10.6342/NTU202402499

economy will contribute to 30% of the global GDP and create 30 million jobs by 2030.[13] Consequently, the adverse trade impacts resulting from data localisation measures could impede long-term global economic prosperity.

Nonetheless, it is essential to recognize that economic concerns should not be the sole focus of governments. There are legitimate reasons for implementing data localisation measures worth consideration. The key inquiry revolves around distinguishing between legitimate justifications for imposing such measures and those that are not and finding a balance between upholding these legitimate objectives while mitigating the trade-restrictive consequences of data localisation on a global scale.

B. WTO as The Only Multilateral Trade Forum to Address Trade Issues

Although there is an arising number of rules that restrict data localisation measures in the context of Regional Trade Agreements (hereinafter "RTAs") or Digital Economy Agreements (hereinafter "DEAs"),[14] the international society has no consensus on whether and how data localisation measures shall be restricted when they become barriers to trade. Studies demonstrate that data localisation measures can lead to trade and productivity losses due to their restrictive impact on data flow.[15] Therefore, it becomes imperative to address the negative trade impact resulting from such measures at the multilateral level.

Nowadays, the World Trade Organization (hereinafter "WTO") stands out as the most inclusive institution overseeing multilateral trade affairs,[16] consisting of 164 Members as

[13] Arya Devi, *DCO 2030: Digital Economy to Contribute 30% of Global GDP and Create 30 Million Jobs by 2030*, EDGE (Feb. 5, 2023), https://www.edgemiddleeast.com/business/dco-2030-digital-economy-to-contribute-30-of-global-gdp-and-create-30-million-jobs-by-2030.
[14] CHIARA DEL GIOVANE ET AL., OECD TRADE POLICY PAPERS NO. 278 THE NATURE, EVOLUTION AND POTENTIAL IMPLICATIONS OF DATA LOCALISATION MEASURES 16 (2023).
[15] CORY & DASCOLI, *supra* note 9, at 1
[16] PETER VAN DEN BOSSCHE & WERNER ZDOUC, THE LAW AND POLICY OF THE WORLD TRADE ORGANIZATION 83 (4th ed., 2017).

doi:10.6342/NTU202402499

of July 29, 2016, which encompasses nearly all major players in global trade.[17] While the WTO does not explicitly regulate data localisation measures, some WTO Members have proposed to prohibit such measures during the WTO E-commerce Joint Statement Initiative.[18]

Hence, the WTO may play an essential role in helping the international society mitigate the negative trade impacts of data localisation measures and foster more liberalized data governance polices globally.

II. AIMS OF THE STUDY

This thesis aims to address the compatibility of GATS and local storage requirements which belong to one type of data localisation measures, and to further discuss how the WTO should regulate local storage requirements in the future.

To achieve the said aims, the thesis will conduct the following steps. First, studying the nature and trade impact resulting from local storage requirements. Second, researching measures that are forbidden under the GATS and discussing whether local storage requirements fall within such measures. Third, analyzing whether the WTO members are competent with the current regulatory framework of the WTO laws to address the trade impacts resulting from local storage requirements. Fourth, exploring

[17] *Understanding the WTO: The Organization Members and Observers*, WORLD TRADE ORGANIZATION, https://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm (last visited Apr. 10, 2024).
[18] Joint Statement on Electronic Commerce Initiative: Communication from the United States, WTO Doc. INF/ECOM/5 (Mar. 25, 2019) [hereinafter US JSI Proposal], ¶ 2; Joint Statement on Electronic Commerce Initiative Proposal for the Exploratory Work by Japan, WTO Doc. JOB/GC/177 (Dec. 4, 2018) [hereinafter Japan JSI Proposal], ¶ 3.8 ("As cross-border data transfer becomes an essential part of business practices. Companies take strategic decisions on the locations of computing facilities, taking into account the cost and efficiency of operations, while at the same time hedging various risks. In such contexts, mandatory requirements by a government to locate servers within its territory would discourage companies from entering into its market due to the increased cost and risk associated with such requirements. Therefore, it would be worth considering reaching an agreement among Members in the WTO in which, with the exception of cases to achieve a legitimate public policy objective, governments should not impose mandatory requirements on the location of servers, as such requirements pose critical barriers to entry into the market by foreign businesses.").

doi:10.6342/NTU202402499

alternative regulatory frameworks for local storage requirements in the international trade law regimes. Last but not least, analyzing how WTO should regulate local storage requirements based on the insights drawn from the previous steps.

III. METHODOLOGY

A. Literature Review

This thesis firstly adopts the literature review method to understand how data localization is defined across various literatures and the rationale behind governments implementing such measures. In addition, this method is also applied to explore different forms of data localisation measures identified in literatures and to observe how local storage requirements are implemented in the global landscape.

Additionally, this method helps analyze the controversies surrounding data localisation that scholars have already discussed to further examine the negative trade impacts of local storage requirements that have not been fully addressed. Furthermore, this method is also adopted to realize governments' stances on the prohibition of local storage requirements within the context of the international trade regime.

Given the relatively new concept of data localisation, this thesis consults a wide variety of sources, including books, journals, reports, papers, and online sources which have discussed the controversies of data localisation. Overall, the literature review method aids in understanding how other academics or researchers analyze the negative trade impact resulting from data localization measures and their opinions towards such measures.[19] Building on their observations, this thesis seeks to identify the nature of local

[19] *See* CHRIS HART, DOING A LITERATURE REVIEW: RELEASING THE RESEARCH IMAGINATION 1 (2d ed. 2018).

doi:10.6342/NTU202402499

storage requirements and discover their negative trade impacts that governments may seek to mitigate.

B. Leading Case Study Method

The leading case study method is employed to investigate the compatibility of local storage requirements with the General Agreement on Trade in Services (hereinafter "GATS").[20]

This method helps ascertain how the WTO jurisprudence applies GATS to determine what measures are inconsistent therewith and further explores whether local storage requirements are consistent with these covered agreements.

C. Comparative Method

To gain a deeper understanding of the interplay between trade agreements and local storage requirements, a comparative methodology is adopted. This thesis examines provisions prohibiting data localisation measures within RTAs or DEAs established post-2014. This timeframe is selected because clauses prohibiting data localisation measures emerged after 2014.[21]

Specifically, this thesis will study and compare the convergence and divergence of the following RTAs and DEAs: the Trans-Pacific Partnership Agreement, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership, the Digital Economy Partnership Agreement between New Zealand, Singapore, and Chile, and the Regional Comprehensive Economic Partnership.

[20] General Agreement on Trade in Services, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183, 33 I.L.M. 1167 (1994) [hereinafter GATS].
[21] CHIARA DEL GIOVANE ET AL., *supra* note 14, at 18.

doi:10.6342/NTU202402499

IV. SCOPE OF THE RESEARCH

A. Focus on Local Storage Requirements' Trade Impact on Services

It is worth noting that data localisation lacks a universal definition and is sometimes conflated with rules on cross-border data transfer.[22] Therefore, some literature primarily discusses the trade impact of data localisation mainly within the context of restrictions on data flows.[23] Nonetheless, since the concept of data localization fundamentally concerns governmental control of data within a specific geographical region, it should encompass not only measures that restrict cross-border data transfers but also those that mandate data storage or processing within a particular geographical region.[24]

While data localization involves various measures with multifaceted trade impacts, this thesis only focuses on examining the trade restrictiveness of local storage requirements on services. To maintain clarity, the term "local storage requirement" in this thesis refers exclusively to "any laws, regulations or administrative requirements mandating the storage of certain data within a specific geographical location." It does not necessarily encompass requirements for local data processing or imposing limitations on data transfer to other nations.[25]

---

[22] *See* CHIARA DEL GIOVANE ET AL., *supra* note 14, at 6 ("A number of definitions for data localisation have been proposed in the literature, including: "Forced local data-residency requirements that confine data within a country's borders, a concept known as "data localization,"" (Cory and Dascoli, 2021[2]). "We define 'data localization' measures as those that specifically encumber the transfer of data across national borders. These measures take a wide variety of forms—including rules preventing information from being sent outside the country, rules requiring prior consent of the data subject before information is transmitted across national borders, rules requiring copies of information to be stored domestically, and even a tax on the export of data." (Chander and Lê, 2015[6])).

[23] *See* Brad Carr ET AL., *Data Localization: Costs, Tradeoffs, and Impacts Across the Economy,* INST. OF INT'L FINANCE (Dec. 22, 2020), https://www.iif.com/portals/0/Files/content/Innovation/12_22_2020_data_localization.pdf.

[24] *See* CHIARA DEL GIOVANE ET AL., *supra* note 14, at 6 ("A mandatory legal or administrative requirement directly or indirectly stipulating that data be stored or processed, exclusively or non-exclusively, within a specified jurisdiction" (Svantesson, 2020[3])").

[25] *See Id.* at 8 ("The first category of approaches refers to measures that require local storage of data, without prohibiting storage or processing in other countries (Category 1). These measures are often applied in the context of ensuring that regulators do not encounter issues related to jurisdictional reach. Approaches falling

doi:10.6342/NTU202402499

B. Examine the Compatibility of Local Storage Requirements with GATS

This thesis only analyzes the trade barriers of local storage requirements to services, with a primary focus on analyzing the compatibility of such requirements with the GATS. It does not explore potential violations of other WTO agreements such as the General Agreement on Tariffs and Trade (hereinafter "GATT").[26]

V. STRUCTURE OF THE THESIS

The thesis is structured in the following manner. Chapter One is the introduction of the thesis. In Chapter Two, to comprehend the trade implications of local storage requirements on a global scale, this thesis initiates its inquiry by defining and differentiating local storage requirements from the broad meanings of data localisation measures. Based on this understanding, the thesis further examines the implementation of such requirements across various countries.

In Chapter Three, the thesis delves into the compatibility of local storage requirements with the GATS. This analysis explores the trade principles and exceptions that are relevant to local storage requirements in the GATS. After analyzing the compatibility of these mandates with the GATS, this thesis further investigates the current stance of WTO Members on local storage requirements by reviewing the historical trajectory and current status of WTO e-commerce negotiations.

In Chapter Four, this thesis examines the clauses regulating data localisation measures under RTAs and DEAs that have emerged since 2014. This analysis involves an

under this category tend to target business records (accounts), telecommunications or financial data, including in the context of data retention policies. For example, Sweden's Accounting Act stipulates that accounting information is to be retained and stored for seven years in Sweden.").

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

doi:10.6342/NTU202402499

assessment of the nature, extent, and exceptions of these clauses to better understand why certain WTO Members advocate for the prohibition of local storage requirements in their trade agreements.

In Chapter Five, this thesis endeavors to address the question of whether the WTO should address local storage requirements explicitly and propose a draft article that regulates local storage requirements within the WTO framework.

VI. LIST OF ABBREVIATIONS

CPTPP	Comprehensive and Progressive Agreement for TransPacific Partnership
Data Retention Directive	Council Directive 2006/24/EC
DEA	Digital Economy Agreement
DEPA	Digital Economy Partnership Agreement between New Zealand, Singapore, and Chile
EU	European Union
EU-UK TCA	Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the One Part, and the United Kingdom of Great Britain and Northern Ireland, of the Other Part

doi:10.6342/NTU202402499

EFTA-Moldova FTA	Free Trade Agreement between the EFTA States and the Republic of Moldova
EU-New Zealand FTA	Free Trade Agreement between the European Union and New Zealand, EU-New Zealand EU-UK Trade and Cooperation Agreement
FTA	Free Trade Agreement
GATT	General Agreement on Tariffs and Trade
GATS	General Agreement on Trade in Services
GDPR	General Data Protection Regulation
GVCs	Global Value Chains
ICT	Information and Communication Technology
Japan–Mongolia FTA	Agreement Between Japan and Mongolia for an Economic Partnership
JSI	Joint Statement Initiative
LDCs	Least-Developed Countries
MFN	Most-Favoured Nation

doi:10.6342/NTU202402499

No. 242-FZ	Russian Federal Law No. 242-FZ
OECD	Organization for Economic Cooperation and Development
PDPL	Russian Procedure for Personal Data Processing in Information-Telecommunication Networks
RTA	Regional Trade Agreement
RCEP	Regional Comprehensive Economic Partnership
TPP	Trans-Pacific Partnership
Treaty of Lisbon	Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community
USMCA	United States-Mexico-Canada Agreement
WTO	World Trade Organization
WTO Agreement	Marrakesh Agreement Establishing the World Trade Organization

doi:10.6342/NTU202402499

CHAPTER TWO

THE GLOBAL LANDSCAPE OF DATA LOCALISATION REQUIREMENTS

I. WHAT IS DATA LOCALISATION

A. The Definition of "Data Localisation" Varies in Different Literatures

It is worth noting that data localisation lacks a universal definition and may be interpreted differently across various sources. Different literatures have suggested various definitions of data localisation, encompassing: "forced local data-residency requirements that confine data within a country's borders;"[27] "A mandatory legal or administrative requirement directly or indirectly stipulating that data be stored or processed, exclusively or non-exclusively, within a specified jurisdiction;"[28] "Any legal or administrative measure which states that data processing must take place in a specific … territory;"[29] "rules that specifically encumber the transfer of data across national borders."[30]

To avoid confusion arising from diverse interpretations of "data localisation", this thesis defines "data localisation" as "any mandatory legal or administrative requirement

[27] CHIARA DEL GIOVANE ET AL., *supra* note 14, at 5-6 ("A number of definitions for data localisation have been proposed in the literature, including: •"Forced local data-residency requirements that confine data within a country's borders, a concept known as "data localization,"" (Cory and Dascoli, 2021[2]).• "A mandatory legal or administrative requirement directly or indirectly stipulating that data be stored or processed, exclusively or non-exclusively, within a specified jurisdiction" (Svantesson, 2020[3]).• "Any legal or administrative measure which states that data processing must take place in a specific EU territory" – EU Regulation on the free flow of non-personal data. (supra note 1)• "We define 'data localization' measures as those that specifically encumber the transfer of data across national borders. These measures take a wide variety of forms—including rules preventing information from being sent outside the country, rules requiring prior consent of the data subject before information is transmitted across national borders, rules requiring copies of information to be stored domestically, and even a tax on the export of data." (Chander and Lê, 2015[6])• "Data localization has two meanings. The first is a policy whereby national governments compel Internet content hosts to store data about Internet users in their country on servers located within the jurisdiction of that national government (localized data hosting). The data stored in the local jurisdiction may be either the sole copy of the data or a required local copy of data sent for storage or processing in another jurisdiction. The second form of data localization is a policy, whereby national governments compel Internet service providers to route data packets sent between Internet users located in their jurisdictions across networks located only within their jurisdiction (localized data routing)." (Selby, 2017[7])").

[28] *Id.* at 5-6.

[29] *Id.*

[30] *Id.*

doi:10.6342/NTU202402499

directly or indirectly stipulating that data be stored or processed, exclusively or non-exclusively, within a specified jurisdiction."

This definition is chosen because the concerns of data localisation measures mainly involve governments' restriction on data usage within a specific region. Therefore, data localisation should encompass not only measures that restrict cross-border data transfers but also those that mandate data storage or processing within a particular geographical region. Such a definition helps provide a more precise and comprehensive understanding of data localisation related to the domestic regulatory landscape surrounding data governance.

B. Local Storage Requirement

As previously introduced, local storage requirements can be "any laws, regulations or administrative requirements mandating the storage of certain data within a specific geographical location." It does not necessarily encompass requirements for local data processing or imposing limitations on data transfer to other nations. Local storage requirements typically aim to ensure the jurisdictional reach of certain information, such as business records, telecommunications, or financial data, often within the framework of data retention regulations.[31]

For instance, the most common local storage requirements in the European Union (hereinafter "EU") Member states relate to accounting information and financial statements. In Belgium, concerning the VAT, invoices received and copies of invoices issued by the taxpayer must be stored in Belgium or in another EU Member state under

[31] CHIARA DEL GIOVANE ET AL., *supra* note 14, at 8

doi:10.6342/NTU202402499

certain conditions.[32] Germany also shares similar local storage requirements on tax records.[33]

Local storage requirements can be further classified into two main types: (i) general local storage requirements and (ii) sector-specific local storage requirements.[34] General local storage requirements mandate any individual or entity to store sensitive data locally, irrespective of the industry or sector to which their business pertains.[35] For instance, in China, Article 37 of the Cybersecurity Law of the People's Republic of China requires infrastructure operators who gather or produce personal information or important data during operations within China's sovereignty to store those data therein.[36]

On the other hand, specific local storage requirements only apply to specific sectors or industries handling sensitive data on a regular basis, obliging them to comply with local data storage mandates.[37] For instance, in Poland, entities involved in gambling must store real-time data shared between the entity and its users on a storage device located within Poland.[38] Similarly, in India, the Insurance Regulatory and Development Authority dictates that all original records of policyholders should be kept in India.[39]

---

[32] CORY & DASCOLI, *supra* note 9, at 30 ("Belgium … 1992: According to VAT Code – Article 60, VAT invoices must be stored in Belgium or another EU member state").
[33] *Id.* at 32 ("Germany … 2013: According to the Tax Code, persons and firms that are required to keep books and records must keep them within Germany. There are some exceptions for multinational companies.").
[34] *See* Han-Wei Liu, *Data Localization and Digital Trade Barriers: ASEAN in Megaregionalism*, in ASEAN LAW IN THE NEW REG'L ECON. ORD.: GLOB. TRENDS & SHIFTING PARADIGMS 371, at 374 (Pasha L. Hsieh & Bryan Mercurio eds., 2019) ("Type I: Forced Local Data Storage [] Governments in this camp take the strictest stance by requiring data to be stored in facilities physically located within a geographic border … Type II: Sector-Specific Data Storage Requirements [] Countries in this camp subject cross-border data flows to certain requirements, narrowing down the scope of local data storage to selected sectors.").
[35] *Id*.
[36] *Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)*, DIGICHINA (June 29, 2018), https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/.
[37] LIU, *supra* note 34, at 374.
[38] CORY & DASCOLI, *supra* note 9, at 34 ("Poland … 2009: According to the Polish Gambling Act, data on legal gambling activity must be archived in real time on a server in Poland.").
[39] *Id.* at 43 ("India … 2017: The Insurance Regulatory and Development Authority of India mandates that all original policyholder records should be maintained in India and obtain express consent from the data

doi:10.6342/NTU202402499

C. Local Processing Requirements

Local processing requirements mandate data to be processed within a specific jurisdiction.[40] The term "processing" encompasses a broad range of activities, including storage, reuse, and deletion.[41] Because "processing" includes actions more than merely "storing," local processing requirements typically impose greater constraints than local storage requirements.[42] For instance, in Luxembourg, the financial supervision authority requires client data to be stored and processed locally according to Circular CSFF 12/552.[43] This requirement can be deemed a local processing requirement.

Considering local processing requirements require data to be processed within a designated jurisdiction, they typically forbid cross-border data transfers at the same time. Consequently, local processing requirements are regarded as the strictest form of data localisation measures, as they not only mandate data storage and processing within a specific national jurisdiction but also prohibit any data processing outside of it.[44]

Mandating data processing within a designated geographic area often has the same impact as banning cross-border data transfers. However, certain local processing requirements might permit data transfers under specific and well-defined conditions.[45]

---

subject to transfer data outside India.").

[40] Helena Ursic ET AL., *Data Localisation Measures and Their Impacts on Data Science*, in Research Handbook in Data Science and Law 322 (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3102890, at 4 ("Data must be processed within territory under a specified national jurisdiction. Processing has a broad meaning in data protection terminology and covers a wide range of activities, including storage, reuse and deletion. As 'processing' is a broader term than storing, a requirement to ensure local processing will typically be more restrictive than the requirement to store data locally").

[41] *Id.*

[42] Helena Ursic ET AL., *supra* note 40, at 4.

[43] MATTHIAS BAUER ET AL., UNLEASHING INTERNAL DATA FLOWS IN THE EU: AN ECONOMIC ASSESSMENT OF DATA LOCALISATION MEASURES IN THE EU 7 (2016), https://ecipe.org/wp-content/uploads/2016/12/Unleashing-Internal-Data-Flows-in-the-EU.pdf ("According to the Circular CSFF 12/552, financial institutions in Luxembourg are required to process their data within the country. Processing abroad is exceptionally permitted for an entity of the group to which the institution belongs or with explicit consent.").

[44] CHIARA DEL GIOVANE ET AL., *supra* note 14, at 9.

[45] *Id.* at 10.

doi:10.6342/NTU202402499

These kinds of local processing requirements with flow conditions are relatively uncommon. One example is Australia's Personally Controlled Electronic Health Records Act, which mandates that personal health records must be stored solely within Australia.[46] However, this Act permits data to be held and processed outside Australia under certain conditions.[47] These conditions ensure that sensitive information remains protected and that transfers are conducted in a controlled and regulated manner.

To be clear, restrictions on data transfer do not necessarily require local storage or processing of data. Instead, they merely require cross-border data transfers to comply with specific conditions.[48] For instance, although the European Union does not have explicit local storage requirements, it permits cross-border data transfers only if the recipient countries outside the EU can ensure an adequate level of protection.[49]

II. MANDATES OF DATA LOCALISATION

The number of data localisation measures is growing across nations. As of early 2023, nearly 100 data localisation measures were implemented across 40 countries, with over half of them enacted since 2015.[50] Furthermore, data localisation measures are growing

[46] *Id* ("Australia's Personally Controlled Electronic Health Records Act requires that personal health records be stored only in Australia. Nevertheless [,] it foresees the possibility of transfers where the data subject or the registered healthcare provider organisation need access while overseas. Moreover, the Act specifies the following conditions: The System Operator is authorised, for the purposes of the operation or administration of the My Health Record system: a) to hold and take such records outside Australia, provided that the records do not include: i. personal information in relation to a healthcare recipient or a participant in the My Health Record system; or ii. identifying information of an individual or entity; and b) to process and handle such information outside Australia, provided that the information is neither of the following: i. personal information in relation to a healthcare recipient or a participant in the My Health Record system; ii. identifying information of an individual or entity.").
[47] CHIARA DEL GIOVANE ET AL., *supra* note 14, at 10.
[48] LIU, *supra* note 34, at 375 ("countries that follow this model do not "localize" data for they do not mandate local data storage. Nevertheless, as illustrated in the case of the European Union, such an approach could prohibit data from crossing the border. In the European Union, cross-border data flows have long been regulated under the 1995 Data Protection Directive 95/47/EC.20 This directive prohibits personal data from being exported outside the European Economic Area unless third countries maintain "an adequate level of protection," as determined by the European Commission").
[49] Council Directive 95/46, art. 25(1), 1995 (EC).
[50] CHIARA DEL GIOVANE ET AL., *supra* note 14, at 3 ("By early 2023, close to a hundred data localisation measures across 40 countries were in place. More than half of these have emerged since 2015 … By 2023,

doi:10.6342/NTU202402499

more stringent. As of 2023, over two-thirds of these measures mandated local storage and processing without allowing data to leave the country, representing the most stringent type of data localisation requirements.[51] This section presents the common rationales for countries to implement such measures.

A. Data Sovereignty

"Data sovereignty" stems from the historical concept of a state's absolute and exclusive control, known as "sovereignty," within its geographical boundaries. Initially, as a concept proposed by Bodin, sovereignty refers to the ultimate power possessed by a state over its territory and citizens, which encompasses both internal and external dimensions.[52]

Data sovereignty extends this traditional notion of state sovereignty to encompass the control over data flows through national jurisdictions.[53] Many nations enact data localisation policies based on data sovereignty rationale and assert that their sovereignty could be jeopardized if they lack full control over data stored beyond their borders.[54] This assertion reflects a belief that data stored externally may be subject to foreign laws and regulations, potentially compromising national interests or security. Therefore, by mandating that certain data must be stored locally, governments aim to maintain control over sensitive information critical to their sovereignty.

---

more than two thirds of measures in place imposed a local storage and processing requirement without the possibility for data to flow outside the country, the most restrictive form of data localisation identified.").

[51] *Id.*

[52] Paul Timmers, *Sovereignty in the Digital Age*, *in* INTRODUCTION TO DIGITAL HUMANISM 571, at 575 (Hannes Werthner et al. ed., 2023), https://link.springer.com/chapter/10.1007/978-3-031-45304-5_36 ("Bodin (1529) came up with the concept of the sovereign as a person who exercises absolute and undivided power with impact both internal to the state and in the external affairs of the state.").

[53] Patrik Hummel ET AL., *Data Sovereignty: a Review*, 8(1) BIG DATA & SOCIETY 1 (2021), https://journals.sagepub.com/doi/pdf/10.1177/2053951720982012 ("Data sovereignty involves, or can be identified with, the control of data flows via national jurisdiction").

[54] *See generally id.*

doi:10.6342/NTU202402499

B. National Security

National security also emerges as one of the significant political rationales of data localisation policies. Various nations have invoked concerns about national security to justify limitations on digital trade.[55] In particular, certain governments, especially in authoritarian regimes such as China and Russia, assert that maintaining physical access to data centres is vital for enhancing surveillance capabilities and exerting political control.[56]

Some proponents of data localisation policies argue that storing nationally sensitive data within a country's borders ensures its protection. However, critics argue that local storage does not guarantee confidentiality or safety,[57] contending that data security relies more on the server's technical, physical, and administrative controls rather than its location.[58] Moreover, opponents contend that requesting firms and government agencies to adopt best-in-class cybersecurity practices and services can be an alternative to secure data protection and reduce the restriction on data flow at the same time.[59]

Nonetheless, data security and privacy concerns have become a global talking point among governments following the revelations by Edward Snowden who is a former National Security Agency contractor which concerns the disturbing relationship between major U.S. technology firms and the American national security establishment.[60] These

[55] Martina Ferracane, *Data Flows & National Security: a Conceptual Framework to Assess Restrictions on Data Flows Under GATS Security Exception*, 21(1) DIGITAL POLICY REGULATION AND GOVERNANCE 44 (2018), https://deliverypdf.ssrn.com/delivery.php?ID=542020096000010101113085071078065102026044031032057003066126105028004098107024117066031056003008104040034096126065110016013088027091046046045108065111104101080028004077083060021095017078122116080076027015122025125069019075091111086094024092001067000102&EXT=pdf&INDEX=TRUE.
[56] CORY & DASCOLI, *supra* note 9, at 7.
[57] *Id.* at 5.
[58] *Id.*
[59] *Id.*
[60] JONAH FORCE HILL, THE GROWTH OF DATA LOCALIZATION POST-SNOWDEN: ANALYSIS AND RECOMMENDATIONS FOR U.S. POLICYMAKERS AND BUSINESS LEADERS 5 (2014),

doi:10.6342/NTU202402499

revelations have heightened many countries' awareness of the potential threats to their national security from data leaks.[61] Germany's response mirrors the fundamental character of a nation-state to assert control over its territory, including data within its borders. Therefore, the urge to preserve national security, heightened by concerns of foreign spying, has further incentivized the implementation of data localisation requirements.

C. Law Enforcement and Regulatory Oversight

It is also believed that data localisation can ensure the accessibility of data necessary for domestic law enforcement.[62] Given that the enforcement jurisdiction is typically territorial-based, obtaining data beyond its territory may present challenges.[63]

For example, Google turned down a request from the Brazilian government in 2024 to obtain information related to several cases pending in the Brazilian Supreme Court.[64] This incident highlights the challenges governments face in obtaining data necessary for law enforcement from outside their jurisdictions.

Similarly, India has repeatedly requested the US Government to issue summonses to Google, Facebook, Twitter, and others for not stopping the spread of speech that is banned under Indian Law. However, these requests were declined due to concerns about US civil liberties.[65]

---

https://deliverypdf.ssrn.com/delivery.php?ID=267119122101065066121087011084028077034092086004057035102124027103105105076070109087038017120036122008044071099013103011001103009046056035086102126127017083121027125034021008121099029082120118002003099076119002095030092087115118100004005118127013012068&EXT=pdf&INDEX=TRUE.

[61] Alison Smale, *Merkel Backs Plan to Keep European Data in Europe*, THE N.Y. TIMES (Feb. 16, 2014), http://www.nytimes.com/2014/02/17/world/europe/merkel-backs-plan-to-keep-europeandata-in-europe.html?hp&_r=0.

[62] Helena Ursic ET AL., *supra* note 40, at 11.

[63] *Id.*

[64] Helena Ursic ET AL., *supra* note 40, at 12.

[65] *Id.*

doi:10.6342/NTU202402499

Another significant example is the *United States v. Microsoft Corp.*, which illustrates the legal difficulties associated with accessing data located outside one's borders.[66]

Due to the difficulties of accessing data from foreign jurisdictions, data localisation policies have been deemed as a means to facilitate the application of local law.[67] For instance, the Indian government proposed a data protection bill in 2019 and declared that securing faster and better access to personal data for law enforcement is one of the key objectives for data localization.[68] This is particularly the case if considering that it had suffered from difficulties in accessing personal data for national security and law enforcement purposes.[69]

However, the transnational nature of crime and digital services necessitates international cooperation even when data localisation measures are in place.[70] Therefore, some critics argue that the law enforcement objective is sustained mainly because policymakers do not want to improve the process of making cross-border requests.[71]

D. Data Protection and Personal Privacy

As the internet prospers, ensuring data protection and personal privacy has become increasingly challenging. Within this context, data localisation rules can arise as a country's effort to protect personal data and the right to privacy.[72] For instance, Europe

[66] Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016); *See* United States v. Microsoft Corp., 584 U.S. ___, 138 S. Ct. 1186 (2018) (This case concerning whether an email provider who has been served with a warrant required, under 18 U.S.C. § 2703, should provide the federal government with emails, even when the email records are stored exclusively outside the United States. In this case, Microsoft challenged a subpoena granted to the US government for accessing their data stored on an Irish server. The case was appealed and heard by the Supreme Court, and then the judgment was remanded and eventually dismissed).
[67] Helena Ursic ET AL., *supra* note 40, at 11.
[68] COMMITTEE OF EXPERTS UNDER THE CHAIRMANSHIP OF JUSTICE B.N. SRIKRISHNA, A FREE AND FAIR DIGITAL ECONOMY PROTECTING PRIVACY, EMPOWERING INDIANS (July 27, 2018), at 88, https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.
[69] *See Id.* at 89-90.
[70] CORY & DASCOLI, *supra* note 9, at 9.
[71] *Id.*
[72] TOBIAS NAEF, DATA PROTECTION WITHOUT DATA PROTECTIONISM: THE RIGHT TO PROTECTION OF PERSONAL DATA AND DATA TRANSFERS IN EU LAW AND INTERNATIONAL TRADE LAW 1 (2023),

doi:10.6342/NTU202402499

has been a forefront advocate of data protection and personal privacy, introducing the General Data Protection Regulation (hereinafter "GDPR") in 2016.[73] Although GDPR does not require EU Member states to store personal data within the EU, Article 45 GDPR imposes restriction on data transfer outside the EU, requiring that any transfer of personal data to a third country or an international organization may only take place when an adequate level of data protection is ensured.[74]

In addition, sensitive personal data is usually subject to local storage requirements or local processing requirements. For instance, in 2012, Australia's Personally Controlled Electronic Health Records Act enacted by Australia requires that personal health records be stored only in Australia.[75]

E. Geopolitical Risks and Financial Sanctions

Countries may impose data localisation rules to reduce the risks associated with international financial sanctions. Data localisation requirements imposed on payment services may be deemed to facilitate the establishment of national payments to mitigate geopolitical and sovereign risks resulting from the reliance on global payment networks.[76] For instance, after the international sanctions occurred in 2014, which forced Visa and Mastercard to end services in Russia, Russia then required payment data localisation to build its national payment system named MIR.[77]

Although the occurrence of international financial sanctions is rare, Indonesia, Mexico, South Africa, and Vietnam still impose payment services-related restrictions.[78]

---

https://doi.org/10.1007/978-3-031-19893-9_6.
[73] *Id.* at 116; *see generally* General Data Protection Regulation, 2016 O.J. (L 119) 1 [hereinafter GDPR].
[74] *Id.* at 127.
[75] *My Health Records Act 2012* div 1 s 17 (Austl.) [hereinafter My Health Records Act].
[76] NAEF, *supra* note 72, at10.
[77] *Id.*
[78] *Id.*

doi:10.6342/NTU202402499

For example, the South African Reserve Bank imposes a moratorium on the planned migration of the processing of card transactions offshore.[79] South African Reserve Bank deemed that the sole reliance on offshore processing of domestic transactions may result in potential sovereign, geopolitical, and financial stability risks to South Africa.[80]

F. Economic Protectionism

Data innovation, which involves utilizing data to generate value, has become increasingly important to economic growth, competitiveness, scientific discovery, and social progress as new technologies and methods have made it easier to collect, store, analyze, share, and use information.[81] Therefore, an increasing number of policymakers are leveraging data to give an advantage to domestic companies.

It is recognized that a small number of corporations, such as Google, Amazon, Apple, Facebook, and Microsoft, wield considerable control over data globally.[82] However, in terms of hosting locations, 42 percent of the world's top million sites are based in the United States (hereinafter "US") and Canada, 31 percent in Europe, and only a mere 12 percent in the Asia Pacific region, with the rest scattered across other parts of the world.[83]

Various measures are being implemented to address these disparities, ranging from advocating for stricter regulation of the technology sector to considering data localisation

---

[79] *Id.*

[80] SOUTH AFRICAN RESERVE BANK NATIONAL PAYMENT SYSTEM DEPARTMENT, CONSULTATION PAPER PROCESSING OF PAYMENTS IN SOUTH AFRICA (Nov. 2018), https://financedocbox.com/Insurance/114473644-National-payment-systemdepartment-consultation-paper-processing-of-payments-in-south-africa.html.

[81] Daniel Castro & Travis Korte, *Data Innovation 101*, CTR. FOR DATA INNOVATION (Nov. 3, 2013), https://www.datainnovation.org/2013/11/data-innovation-101/.

[82] David Parkins, *The World's Most Valuable Resource is No Longer Oil, but Data,* THE ECONOMIST (May. 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (last visited Apr. 10, 2024).

[83] James Manyika ET ALT., *Digital Globalisation: The New Era of Global Flows*, MCKINSEY GLOB. INST. (Feb. 24, 2016), https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows.

doi:10.6342/NTU202402499

as a strategy to boost the domestic industry. For instance, the initial version of India's Non-Personal Data Governance Framework included a proposal to compel companies to share anonymized datasets, presumably to assist local businesses.[84] Similarly, the Srikrishna Committee's report highlights the "positive impact of server localisation on the creation of digital infrastructure and industry."[85]

Nonetheless, critics assert that the costs of data localisation actually outweigh its economic benefits. In a study conducted to quantify the expected losses from data localisation requirements and related measures in seven jurisdictions, researchers found that imposing economy-wide data localisation requirements could reduce countries' GDP and concluded that "any gains stemming from data localisation are too small to outweigh losses in terms of welfare and output in the general economy."[86]

G. Mandates for Local Storage Requirements?

When literature addresses the mandates of data localization measures, it seldom delves into the specific rationales for imposing local storage requirements. Therefore, this thesis examines the precise reasons why countries implement local storage requirements, building on the previously identified rationales for data localization.

Local storage requirements come in both exclusive and non-exclusive forms. Exclusive requirements require targeted data to be stored locally and forbid any copy of such data to be stored abroad. On the other hand, non-exclusive requirements only request a copy of targeted data to be stored locally without restricting cross-border data transfer.

---

[84] Hunton Andrews Kurth, *India Releases Revised Non-Personal Data Framework*, NAT'L L. REV: HUNTON ANDREWS KURTH' PRIVACY AND CYBERSECURITY BLOG (Jan. 15, 2021), https://www.natlawreview.com/Art./india-releases-revised-non-personal-data-framework.

[85] Angelina Dash, *Big Tech vs News Publishers: A Rights-Based Perspective*, CTR. FOR COMMC'N GOVERNANCE BLOG (Sep. 14, 2023), https://ccgnludelhi.wordpress.com/category/internet-governance/.

[86] MATTHIAS BAUER ET ALT., THE COSTS OF DATA LOCALISATION: FRIENDLY FIRE ON ECONOMIC RECOVERY 2(2014), http://www.ecipe.org/app/ uploads/2014/12/OCC32014 1.pdf.

doi:10.6342/NTU202402499

a. Exclusive Local Storage Requirements' Mandates

This thesis contends that the imposition of exclusive local storage requirements may be driven by considerations of data sovereignty, national security, data protection and personal privacy, and economic protectionism. Such requirements prohibit any copy of the targeted data from being stored outside the jurisdiction where they are enforced. In other words, countries implementing these requirements seek to regulate cross-border data flows at the same time.

As mentioned previously, data sovereignty mandate stems from the concerns that countries' sovereignty could be jeopardized if they lack full control over data stored beyond their borders. This concern also encompasses national security rationale, as there is a risk that data containing national secrets or sensitive information stored externally could potentially jeopardize national interests or security.

Data protection and personal privacy can also serve as a basis for exclusive local storage requirements. As previously noted, Australia's Personally Controlled Electronic Health Records Act mandates that personal health records be stored exclusively within Australia. Due to the highly sensitive nature of personal health information, countries may prohibit such data from being stored outside their jurisdiction to mitigate the risk of data leakage.

Additionally, economic protectionism can be a motive for these requirements, particularly when non-exclusive local storage could already provide the same level of protection. Developing countries may view the imposition of exclusive local storage requirements as opportunities to facilitate their domestic industries.

b. Non-Exclusive Local Storage Requirements' Mandates

doi:10.6342/NTU202402499

Non-exclusive local storage requirements can ensure governmental access to targeted data. Consequently, law enforcement mandates are among the most common rationales for countries to impose these requirements. As previously discussed, countries frequently encounter challenges when attempting to access data stored outside their jurisdiction. Thus, ensuring data accessibility is a legitimate concern that motivates governments to impose non-exclusive local storage requirements.

III. LOCAL STORAGE REQUIREMENTS AROUND THE WORLD

Even though the rationales underlying data localisation policies may be controversial, the number of countries that impose data localisation requirements has significantly increased from 35 in 2017 to 62 in 2021.[87] This section presents local storage requirements that have been imposed in different countries, providing a broad global landscape of data restrictiveness levels.

A. Local Storage Requirements in the EU and Its Member States.

a. Accounting Information and Financial Statements

The prevalent local data storage requirements in EU Member countries typically pertain to accounting data and financial records. For instance, in Germany, where all documentation, including invoices, books, accounting records, and business correspondences, must be stored within the country, although certain exceptions apply.[88]

Regarding accounting documents and financial records, Denmark mandates that such records be stored either within Denmark or within the Nordic countries.[89] Similarly, Finland's Accounting Act stipulates that a duplicate of accounting records must be

[87] CORY & DASCOLI, *supra* note 9, at 3.
[88] MATTHIAS BAUER ET AL., *supra* note 43, at 5.
[89] *Id.* at 6.

doi:10.6342/NTU202402499

maintained within Finland.[90] In Sweden, certain documents like a company's annual reports, balance sheets, and annual financial reports are obligated to be physically stored within Sweden for a duration of seven years, with financial services providers practically obliged to house all records within Swedish jurisdiction.[91]

b. Gambling Sectors.

Gambling is another common area where local storage requirements are enforced in the EU. These requirements are in place in three European countries: Bulgaria, Poland, and Romania.[92] For instance, in Bulgaria, individuals applying for a gaming license must ensure that all data related to operations within Bulgaria is preserved on a server located within the country.[93]

Under the Polish Gambling Act, any entity conducting gambling activities must archive in real time all data exchanged between such entity and users on a storage device located in Poland.[94] Additionally, the Act stipulates that servers for processing and storing information and data pertaining to bets and participants must be installed and maintained within the territory of an EU Member state or EFTA.[95]

In Romania, the game server is required to store all data associated with the provision of remote gambling services, encompassing records and player identifications, placed stakes, and payouts. This information must be stored using data storage equipment situated within Romanian territory.[96]

c. The Insights from the Invalid Council Directive 2006/24/EC

[90] *Id.* at 7.
[91] *Id.*
[92] MATTHIAS BAUER ET AL., *supra* note 43, at 5.
[93] *Id.*
[94] MATTHIAS BAUER ET AL., *supra* note 43, at 7.
[95] *Id.* at 19.
[96] MATTHIAS BAUER ET AL., *supra* note 43, at 7.

doi:10.6342/NTU202402499

When EU Member states impose local storage rules, they need to comply with the EU law due to their obligations under the Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community (hereinafter "Treaty of Lisbon").[97] The Court of Justice first addressed the compatibility of a general obligation to retain data with EU law in 2010 by examining the validity of the Council Directive 2006/24/EC, known as the Data Retention Directive. This 2006 regulation required EU Member states to store citizens' telecommunications data for 6 to 24 months,[98] allowing police and security agencies to access details like IP addresses and usage times of all emails, phone calls, and text messages without court permission.

The mandate of the Data Retention Directive seeks to standardize the obligations of public electronic communications service providers across EU Member States regarding data retention and ensure that certain data generated or processed by these providers are available for investigating, detecting, and prosecuting serious crimes as defined by each Member State's national law.[99] Nonetheless, the extensive data retention requirements of the Data Retention Directive sparked significant worries about its adherence to the proportionality principle. These uncertainties prompted the Court of Justice to deliver a verdict in the *Digital Rights Ireland* case, marking the first time the Court declared a broad data retention obligation incompatible with EU law.[100]

Although the Court recognized the importance of ensuring public security, which was one of the objectives of such Directive,[101] it stressed that due to the respect for the right

[97] Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, Dec. 13, 2007, 2007 O.J. (C306) 1 [hereinafter Treaty of Lisbon].
[98] Council Directive 2006/24/EC, art. 6, 2002/58/EC, [2006] O.J. L 105/54.
[99] *Id.* art. 1.
[100] Joined Cases C-293/12 & C-594/12, Digital Rights Ireland Ltd v Minister for Commc'n, Marine and Natural Resources, ECLI:EU:C:2014:238 (June 10, 2014) [hereinafter Digital Rights Ireland].
[101] Digital Rights Ireland, ¶ 51 ("As regards the necessity for the retention of data required by Directive 2006/24, it must be held that the fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may

doi:10.6342/NTU202402499

to privacy and the right to protection of personal data protected by Article 8(1) and Article 7 of the Charter, derogations must be limited to what is strictly necessary.[102] However, the court did not find a real connection between the directive and the public security objectives and therefore concluded that a general obligation of data retention imposed by the Data Retention Directive breached the principle of proportionality and was therefore invalid.[103]

The *Digital Rights Ireland* Case explicitly indicated the limitation of imposing data retention policies within the EU. That is, no Member states' data retention policies shall be applied in a manner inconsistent with the spirit of the right to privacy and the right to protection of personal data, which are fundamental rights protected by the EU charter. Therefore, when EU Member states impose local storage rules, they must comply with these fundamental rights.

B. US - Local Storage Requirements Related to Governments' Data

depend to a great extent on the use of modern investigation techniques. However, such an objective of general interest, however fundamental it may be, does not, in itself, justify a retention measure such as that established by Directive 2006/24 being considered to be necessary for the purpose of that fight.").

[102] Digital Rights Ireland, ¶ 52 ("So far as concerns the right to respect for private life, the protection of that fundamental right requires, according to the Court's settled case-law, in any event, that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (Case C-473/12 IPI EU:C:2013:715, paragraph 39 and the case-law cited).").

[103] Digital Rights Ireland, ¶¶ 57-59 ("In this respect, it must be noted, first, that Directive 2006/24 covers, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime. Directive 2006/24 affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Furthermore, it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy. Moreover, whilst seeking to contribute to the fight against serious crime, Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences").

doi:10.6342/NTU202402499

As previously introduced in Chapter One, Section II, national security is one of the most prevalent rationales for implementing data localisation measures. Since 2011, specific federal government agencies in the US, particularly those dealing with defense and intelligence, have mandated the use of a designated U.S.-based cloud service known as GovCloud. This service ensures local data storage and is crucial for handling sensitive workloads that must comply with strict regulatory frameworks such as those set by the Federal Risk and Management Program ("FedRAMP"). [104]

Notably, this local storage requirement is contractual rather than based on legislation. For instance, the FedRAMP includes particular contractual clauses that refer to the U.S. National Institute of Standards and Technology standard SP 800-53. These clauses provide that U.S. government agencies with particular data location requirements are obligated to incorporate contractual provisions specifying the storage location of data-at-rest, encompassing both primary and replicated storage.[105]

C. Local Storage Requirements and Privacy Protection

Some developed countries impose local storage requirements due to personal privacy protection, which often relates to personal data. This subsection presents the existing implementations of such requirements in Canada and Australia.

a. Canada

In Canada, local storage policies are mainly adopted for data privacy protection mandates. Following the terrorist attacks of September 11, 2001, the US enacted the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 which extended existing legislation to allow high-

[104] CORY & DASCOLI, *supra* note 9, 56.
[105] *Id.*

doi:10.6342/NTU202402499

ranking FBI officials to request a covert court order.[106] This move sparked considerable debate among privacy advocates and some Canadian provincial government officials, who expressed concern that such an Act could be used to access data on Canadian citizens without their awareness or approval.[107]

In response, the British Columbia Legislative Assembly passed Bill 73, also known as the Freedom of Information and Protection of Privacy Amendment Act, 2004, mandating that public bodies ensure that personal information under their control or custody is stored and accessed exclusively in Canada.[108] In 2006, Nova Scotia, another province in Canada, enacted its Personal Information International Disclosure Protection Act, which includes similar stipulations.[109]

b. Australia

In 2012, Australia's Personally Controlled Electronic Health Records Act requires personal health records to be stored exclusively in Australia.[110] However, this Act permits data to be held and processed outside Australia under certain conditions.[111] Accordingly, this Act encompasses the legal approaches of both local storage and local processing requirements, albeit with certain conditions allowing cross-border transfers.

D. Data Localisation Measures in Authoritarian Regimes

Ensuring national security, personal privacy, and law enforcement are frequently cited as legitimate reasons for enforcing local storage mandates. However, in some instances,

---

[106] Fred H. Cate, *Provincial Canadian Geographic Restrictions on Personal Data in the Public* (2008), HUNTON ANDREWS KURTH LLP, https://www.huntonak.com/files/Publication/2a6f5831-07b6-4300-af8d-ae30386993c1/Presentation/PublicationAttachment/0480e5b9-9309-4049-9f25-4742cc9f6dce/cate_patriotact_white_paper.pdf.
[107] *Id.*
[108] *Id.*
[109] *Id.*
[110] CORY & DASCOLI, *supra* note 9, at 54.
[111] CHIARA DEL GIOVANE ET AL., *supra* note 14, at 10.

doi:10.6342/NTU202402499

countries may exploit these justifications as a pretext for censorship. This section delves into the imposition of local storage requirements in authoritarian regimes such as China and Russia, both known for their stringent censorship practices.

a. China

There has been a growing inclusion of data localisation stipulations in Chinese laws and regulations. This is a move by the Chinese government to diminish potential obstacles to its authority over data, and these requirements are dispersed across numerous sector-specific regulations.[112]

Chinese policymaking often provides only high-level requirements. [113] As a result, a unique aspect of China's legal approach is the existence of numerous recommended best practices or standards that are effectively mandatory requirements in practice.[114] These measures are prevalent in sectors like banking, insurance, credit investigation, population health, and genetic information etc.[115]

The first formal local storage requirement emerged in 2011, mandating the storage of the People's Bank of China's financial information within the country's borders.[116] Subsequently, with the introduction of the first national Cybersecurity Law (CSL) in 2016, China aimed to standardize regulations amidst a fragmented landscape.[117] Article

---

[112] Timothy Stratford & Yan Luo, *3 Ways Cybersecurity Law in China is About to Change*, LAW360 (May 2, 2016),
https://www.cov.com/-/media/files/corporate/publications/2016/05/3_ways_cybersecurity_law_in_china_is_about_to_change.pdf.

[113] LILIYA KHASANOVA & KATHARIN TAI, AN AUTHORITARIAN APPROACH TO DIGITAL SOVEREIGNTY? RUSSIAN AND CHINESE DATA LOCALISATION MODELS (July 31, 2023), at 8, https://deliverypdf.ssrn.com/delivery.php?ID=808067068026071070068110001112066091035019070001075003096098086108083015105030002002106039102104013096111076012027070066115098126080022051012092119090071085080126030093028080092101002099075114026070101122092002123122030020006091102110000083100127085023&EXT=pdf&INDEX=TRUE.

[114] CORY & DASCOLI, *supra* note 9, at 49.

[115] *Id.*

[116] LILIYA KHASANOVA & KATHARIN TAI, *supra* note 113, at 8.

[117] *Id.*

doi:10.6342/NTU202402499

37 of the Cybersecurity Law, [118] particularly, introduced a more comprehensive framework, mandating that "personal information" and "other important data" collected or generated within mainland China by "critical information infrastructure operators" (CII operators) must be stored within the country's borders. The terms "other important data" and "CII operators" are broadly defined, encompassing a wide range of information and businesses operating in key sectors such as communication, finance, energy, and transportation. This phase of law consolidation continued with the enactment of the Data Security Law (DSL) and the Personal Information Protection Law (PIPL) in 2021, which provided further clarity on data governance, including localisation requirements.[119]

b. Russia

In 2014, Russian Federal Law No. 242-FZ, which amends certain legislative acts of the Russian Federation, mandates the localisation of personal data.[120] Being one of the earliest and most clear-cut localisation laws that has gained widespread attention, it stands as a prime example of a standard localisation law in Russia.

The stated objective of this data localisation initiative is to halt the unregulated use of data in foreign countries and enhance the safeguarding of the personal data of Russian citizens.[121] This new law amended the Federal Law on Personal Data which stipulates that "[w]hen collecting personal data, including the use of the information and telecommunication network 'the Internet', the operator is required to procure recording, systematisation, accumulation, storage, rectification (update, alteration), retrieval of

[118] *Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)*, DIGICHINA (June 29, 2018), https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/.
[119] LILIYA KHASANOVA & KATHARIN TAI, *supra* note 113, at 9.
[120] Helena Ursic ET AL., *supra* note 40, at 15.
[121] *Id.*

doi:10.6342/NTU202402499

personal data of Russian citizens with the use of databases located in the territory of the Russian Federation . . .”[122]

A literal interpretation of the aforementioned provision might imply that it pertains to any organization handling the data of Russian citizens and that the data localisation stipulation forbids the processing of personal data of Russian citizens in foreign nations.[123] However, the authorities have indicated that the data localisation requirement will primarily apply to websites that cater to Russian citizens and businesses that incorporate Russia into their business strategies.[124] The criteria used to classify a website as “targeted” include the use of a domain name associated with Russia (.ru, .рф, .su, .москва, .moscow, etc.) and the presence of a Russian language version of the website.[125] However, merely having a Russian language version may not be enough to determine that a website is aimed at Russia. In such cases, the Federal Ministry for Communications recommends considering additional factors such as processing payments in rubles, offering a service in Russia (like delivering goods in Russia or using online content in Russia), and displaying advertisements in the Russian language.[126]

For example, the head of Roskomnadzor has stated that the authority currently has no queries for Netflix because its website does not provide a Russian language version.[127] In addition, the authorities clarified that the new data localisation requirement does not forbid the cross-border transfer of data from Russia. It is generally understood that the data of Russian citizens can be processed in other countries, provided that the data is

[122] KPMG, *The Localisation of Russian Citizens' Personal Data: Compliance with the Russian Law on Personal Data* (Sep. 2018), ADV-factsheet-localisation-of-russian-personnal-data-uk-LR.pdf (kpmg.com).
[123] Helena Ursic ET AL., *supra* note 40, at 16.
[124] *Id.*
[125] *Id.*
[126] Helena Ursic ET AL., *supra* note 40, at 16.
[127] *Id.*

doi:10.6342/NTU202402499

initially stored in data centres located in Russia and that these "master" databases are consistently kept up-to-date.[128]

E. Local Storage Requirements in India

Several Indian regulations necessitate the local storage of data. The "National Data Sharing and Accessibility Policy" was implemented by India in 2012, requiring government data to be housed in domestic data centres.[129] The Indian Companies (Accounts) Rules law of 2014 stipulates that if financial data is primarily stored overseas, backups must be kept in India.[130] In 2017, the Insurance Regulatory and Development Authority of India required that all original records of policyholders should be kept in India, and explicit permission from the data subject is needed to transfer data overseas.[131]

In addition, the Ministry of Electronics and Information Technology issued a set of guidelines for government departments regarding contractual terms associated with cloud services.[132] These guidelines stipulate that all government contracts must include a clause for localisation, which mandates that all government data stored in cloud networks must be stored on servers located within India.[133]

In 2018, the Reserve Bank of India implemented regulations that required all payment data to be stored within India.[134] The bank emphasized the necessity for "continuous monitoring and surveillance" of payment data to minimize the risk of data breaches, ensuring that payment services adhere to the highest global cybersecurity standards.[135]

---

[128] *Id.*
[129] NATIONAL DATA SHARING AND ACCESSIBILITY POLICY, https://dst.gov.in/national-data-sharing-and-accessibility-policy-0 (last visited Apr. 10, 2023).
[130] Companies (Accounts) Rules 2014, 2014, Rule 3(5) (India).
[131] CORY & DASCOLI, *supra* note 9, at 43.
[132] *Id.* at 42.
[133] *Id.* at 43.
[134] STORAGE OF PAYMENT SYSTEM DATA (Apr. 6, 2018), https://www.rbi.org.in/commonperson/english/scripts/FAQs.aspx?Id=2995 (last visited Apr. 10, 2024).
[135] Nigel Cory, *Comments on India's Draft National E-Commerce Policy*, Info. Tech. & Innovation Found.

doi:10.6342/NTU202402499

While there are no restrictions on processing payment transactions outside of India, the data must be stored exclusively in India post-processing. If the processing occurs overseas, the data must be erased from foreign systems and returned to India within one business day or 24 hours from the time of payment processing, whichever is sooner.[136]

F. Local Storage Requirements in Southeast and Northeast Asia

a. Indonesia

Indonesian Regulation 69/POJK.05/2016 requires insurers/reinsurers to establish data centres and disaster recovery centres in Indonesia by 12th October 2017.[137] In 2021, the Ministry of Communication and Information Technology in Indonesia released Ministerial Circular No. 3/2021. This circular pertains to the utilization of third-party cloud services by central government agencies for the fiscal year 2021. It establishes 13 security standards that public agencies can apply when using third-party cloud providers. Among these standards are the requirements that providers must have a minimum of two availability zones located at separate data centres within Indonesia and that encryption keys must be stored domestically in Indonesia.[138]

b. South Korea

In 2016, amendments were made to Korea's Regulation on Supervision of Electronic Financial Transactions, permitting financial institutions to utilize cloud services. However, the Financial Services Commission explicitly mandates that such data must be

(Mar. 8, 2019), https://itif.org/publications/2019/03/08/comments-indias-draft-national-e-commerce-policy.

[136] STORAGE OF PAYMENT SYSTEM DATA (Apr. 6, 2018), https://www.rbi.org.in/commonperson/english/scripts/FAQs.aspx?Id=2995 (last visited Apr. 10, 2024).

[137] *The OJK Issues Regulation on Implementation of Insurance and Reinsurance Companies*, GLOBAL BUSINESS GUIDE INDONESIA (Jan. 19, 2017), http://www.gbgindonesia.com/en/main/legal_updates/the_ojk_issues_regulation_on_implementation_of_insurance_and_reinsurance_companies.php.

[138] CORY & DASCOLI, *supra* note 9, at 45.

doi:10.6342/NTU202402499

stored on servers situated within Korea.[139] Furthermore, in 2019, Korea's Cloud Security Assurance Program (CSAP), which oversees cloud services for public sector agencies, stipulated that the physical location of the cloud system and data must be exclusively within Korea.[140]

c. Vietnam

The origins of data localisation regulations in Vietnam can be traced back to Decree 72 issued on July 15, 2013, with subsequent revisions in 2018. Decree 73 mandates that social media platforms must maintain a server system within Vietnam. Additionally, entities that use Vietnamese information infrastructure or have over one million monthly internet users, are required to establish a local branch in Vietnam and store data within the country.[141]

In August 2022, the Vietnamese Government issued Decree 53/2022, which provides guidance on data localisation requirements in the country. This decree is expected to make the general data localisation requirement, as stated in Article 26.3 of the Law on Cyber Security 2018 (LCS 2018), enforceable in practice from 1 October 2022. The decree introduces two key measures for data localisation. Firstly, the storage requirement mandates that all enterprises, both domestic and foreign, must store localized data within Vietnam; and secondly, the local presence requirement stipulates that foreign enterprises must establish a representative office or a branch in Vietnam.[142] The decree allows

[139] *Id.* at 47.
[140] *Id.*
[141] Sanghyun Han, *Data and Statecraft: Why and How States Localize Data*, 26(2) BUSINESS AND POLITICS 263 (2024), at 273, https://www.cambridge.org/core/services/aop-cambridge-core/content/view/386CF1EB4334D28D9C085DF7410EE592/S1469356923000411a.pdf/data-and-statecraft-why-and-how-states-localize-data.pdf.
[142] *Decree 53/2022 - Further Guidance on Data Localisation in Vietnam*, VIETNAM BUS. L., https://vietnam-business-law.info/blog/2022/9/4/decree-532022-further-guidance-on-data-localisation-in-vietnam (last visited Apr. 10, 2024).

doi:10.6342/NTU202402499

enterprises to determine the form of storage, providing them with considerable flexibility. However, it remains unclear whether the data must be stored in a format readable by the authority or if it can be stored in an encrypted or non-electronic form.[143]

Article 26.1 of Decree 53/2022 requires three types of data to be stored in Vietnam: First of all, data relating to personal information of service users in Vietnam, which includes information used to identify an individual; secondly, data generated by service users in Vietnam, which includes account names, service usage time, credit card information, email addresses, IP addresses of most recent login/logout, and the registered telephone number associated with the account or data; thirdly, data on the relationship of service users in Vietnam, which includes friends and groups with whom users connect or interact.[144]

G. Local Storage Requirements in the Middle East and North Africa

a. Algeria

In 2018, Algeria enacted a law that mandates e-commerce platforms operating in the country to register with the government and to host their websites from a data center situated within Algeria.[145]

b. Saudi Arabia

In 2018, the National Cybersecurity Authority of Saudi Arabia stated in its Essential Cybersecurity Controls framework that when using cloud computing services, data hosting and storage must be situated within the country.[146] In 2020, the National Data Management Office of Saudi Arabia issued the National Data Governance Interim

[143] *Id.*
[144] *Id.*
[145] CORY & DASCOLI, *supra* note 9, at 39.
[146] *Id.* at 40.

doi:10.6342/NTU202402499

Regulations, which mandate companies to store and process personal data within the boundaries of Saudi Arabia to ensure the preservation of the country's digital sovereignty over such data.[147]

H. Local Storage Requirements in Africa

In 2011, the Central Bank of Nigeria implemented a regulation requiring entities involved in point-of-sale (POS) card services to store and process data locally.[148] In 2015, Nigeria implemented extensive data localisation requirements under the Guidelines for Nigerian Content Development in ICT, which mandate ICT companies to store all subscriber, consumer, and government data within the country.[149]

In addition, Rwanda implemented a regulation in 2012 stipulating that all crucial government information data, including website hosting email hosting, shared applications like document management and e-archiving, and enterprise applications, must be hosted in the country's national data center.[150]

I. Local Storage Requirements in South and Central America

In 2018, Brazil's Ministry of Planning issued guidelines for government contracts concerning information and communications, which stipulated that confidential data or information managed or produced by the Federal Public Administration, including backup data, must be physically situated within Brazil.[151]

In 2020, Chile's financial regulatory authorities updated regulations detailed in Chapter 20-7 of the Updated Compilation of Banking Standards, mandating that

[147] *Id.* at 39.
[148] *Id.* at 28.
[149] *Id.* at 28.
[150] *Id.* at 29.
[151] *Id.*

doi:10.6342/NTU202402499

"significant" or "strategic" outsourced data must be retained within Chile. Circular No. 2, directed towards non-banking payment card issuers and operators, reiterated similar local storage requirements, potentially encompassing any sensitive records.[152]

In Venezuela, regulations also stipulate that the IT infrastructure used for payment processing must be located within the country's borders,[153] which imposes a requirement for local storage.

IV. THE NEGATIVE TRADE IMPACT OF LOCAL STORAGE REQUIREMENTS

A. The Trade Impact of Data Localisation Requirements

In a 2021 report conducted by the Information Technology and Innovation Foundation (ITIF), it was found that data localisation policies have adverse effects on trade, productivity, and prices in affected industries.[154] The ITIF develops a model that generates a composite index, referred to as the Data Restrictiveness Linkage (DRL), aimed at evaluating the correlation between downstream industries and the level of data restrictiveness within a country, taking into account the data intensity of these industries.[155] The model further investigates the effects of changes in data restrictions on Total Factor Productivity ("TFP"), Price Value-Added indices ("PVA"), and Gross Output Volumes ("GOVs") at the industry level in each country, using the EU-KLEMS database.[156] The model also executes separate log-linear regression models between DRL and these three economic indicators to estimate the percentage changes in productivity, prices, and trade volumes triggered by changes in a country's data transfer restrictions.[157]

[152] CORY & DASCOLI, *supra* note 9, at 48.
[153] *Id.* at 49.
[154] *Id.* at 1.
[155] *Id.*
[156] *Id.*
[157] *Id.*

doi:10.6342/NTU202402499

The Information Technology and Innovation Foundation (ITIF) employs a multifaceted approach to assess the implications of data restrictiveness on various economic parameters.[158] Firstly, they introduce the Data Restrictiveness Index (DRI), utilizing data from the OECD's Product Market Regulation (PMR) Indicators, which measures data flow restrictions on a scale of 0 to 6.[159] The DRI quantifies the level of data restrictions within a country, with higher values indicating more stringent regulations.[160] To refine their analysis, the ITIF introduces the Data-Intensity Modifier (DIM), which adjusts for industry-specific impacts of data restrictions.[161] This ensures a balanced assessment by considering the connection of each downstream industry with national data restrictiveness.[162]

Their research reveals a negative correlation between DRI and Gross Output Volume, with countries experiencing declines in output as data restrictions tighten.[163] For instance, China's gross output volume decreased by 1.7% from 2013 to 2018 as its DRI increased. Similarly, India witnessed a 7.8% reduction in gross output volume during the same period. Moreover, productivity tends to decrease with increasing data restrictiveness, as evidenced by ITIF's regression models.[164] Countries also experience price surges as their DRI scores rise, impacting consumer prices.[165] For example, China experienced a 0.4% increase in prices from 2013 to 2018.

To address these adverse effects, the ITIF proposes collaborative efforts among countries to establish new standards, regulations, and contracts to tackle issues

158 CORY & DASCOLI, *supra* note 9, at 58.
159 *Id.*
160 *Id.*
161 *Id.* at 60.
162 *Id.*
163 *Id.* at 65 ("table 3: Economic costs of case studies due to changes in DRI").
164 CORY & DASCOLI, *supra* note 9, at 65 ("table 3: Economic costs of case studies due to changes in DRI").
165 *Id.*

doi:10.6342/NTU202402499

surrounding transnational data transfers while promoting the free flow of data.[166] They emphasize the importance of international collaboration in fostering a vibrant digital economy,[167] highlighting the absence of an international platform dedicated to advancing data-related matters.

While this ITIF report does not solely focus on measuring the trade impact of local storage requirement measures but also encompasses data transfer restrictions, it offers valuable insights into anticipating the adverse economic consequences arising from local storage requirement measures, which are commonly regarded as the most stringent form of data localisation measures.

B. Local Storage Requirements and SMEs.

Small and medium enterprises (SMEs) play a crucial role in modern economies, contributing significantly to economic development and serving as a key driver of innovation and job creation.[168] While SMEs make up the majority of businesses globally, their involvement in global trade is comparatively restricted compared to larger corporations when considering their contribution to the overall economy and employment.[169]

Nonetheless, Internet has facilitated SMEs' access to international markets. Studies show that being ICT-enabled is more pronounced for SMEs' involvement in trade than

[166] *Id.* at 26.
[167] *Id.*
[168] Murat Bayraktar & Neşe Algan, *The Importance of SMEs on World Economies*, in INTERNATIONAL CONFERENCE ON EURASIAN ECONOMIES 56 (June 2019) (Selahattin Sarı ET ALT. ed.), at 56, https://www.researchgate.net/publication/345358967_The_Importance_Of_SMEs_On_World_Economie.
[169] Emmanuelle Ganne & Kathryn Lundquist, *The Digital Economy, GVCs and SMEs*, in GLOBAL VALUE CHAIN DEVELOPMENT REPORT 2019: TECHNOLOGICAL INNOVATION, SUPPLY CHAIN TRADE, AND WORKERS IN A GLOBALIZED WORLD 121 (2019), at 121, https://www.wto.org/english/res_e/booksp_e/gvc_dev_report_2019_e_ch6.pdf(last visited Apr. 10, 2024).

doi:10.6342/NTU202402499

large firms, indicating that the influence of being digitally enabled is notably higher for small enterprises than for larger ones.[170]

However, local storage measures may become critical trade barriers to the success of SMEs in international trade. For instance, Pegaxis, a property management platform based in Singapore, faces challenges in expanding its operations to new markets due to data server localisation requirements, which would add significant costs to the company.[171] SMEs such as Pegaxis, which utilize a cloud-based approach with servers dispersed worldwide, would face the necessity of transitioning to alternative service providers to adhere to local data storage regulations. This shift would introduce uncertainties regarding the reliability and quality of the services provided by the new providers.[172]

C. Case Study—E-Payments Services and Cloud Computing Services

SMEs relying on digital tools such as online payment processing and cloud computing services for their expansion may typically face negative downstream effects within the context of local storage requirements, given that such requirements increasingly impede digital services relying on regular data processing. This subsection presents how electronic payment services ("E-Payments Services") and cloud computing services may be negatively affected by local storage requirements.

a. E-Payments Services

E-Payments services play a crucial role in the global economy, particularly in emerging economies.[173] E-Payments services are not only widespread but also essential

[170] *Id.* at 128.
[171] *Id.* at 136.
[172] Ganne & Lundquist, *supra* note 169, at 136.
[173] Abdullah Aldaas, *A Study on Electronic Payments and Economic Growth: Global Evidences,* 7

doi:10.6342/NTU202402499

for governments, corporations, and individuals alike, becoming a necessity in today's interconnected world.[174] Nonetheless, as electronic payments increasingly facilitate transactions across borders, local storage measures led to an overall increase in their cost of operations domestically and transnationally.[175] The compliance costs are particularly severe for operations outside OECD countries, where data localisation requirements are more stringent.[176]

Businesses within this sector typically favor centralized server systems to streamline processing and enhance data security. However, adhering to local storage requirements often entails setting up additional servers, which comes with the added challenge of ensuring the overall integrity and security of the payment network system.[177] Therefore, local storage requirements incur expenses E-Payments services, as maintaining local data copies necessitates duplicating security measures across interconnected payment networks, which results in substantial additional investments in both capital and personnel. [178]

In addition, there are various indirect negative consequences associated with local storage requirements in E-Payments services. They include reduced efficiency due to wider fragmentation and increased complexity of global payment systems, leading to longer waiting times and higher transaction costs for users.[179] Moreover, local storage requirements can compromise the security and reliability of e-payment systems, making

---

ACCOUNTING 409, at 413 (2021), https://www.researchgate.net/publication/347993713_A_study_on_electronic_payments_and_economic_growth_Global_evidences.

[174] *Id.* at 413.

[175] CHIARA DEL GIOVANE ET AL., *supra* note 14, at 22.

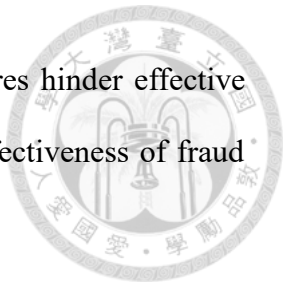
[176] *Id.*

[177] *Id.*

[178] *Id.*

[179] CHIARA DEL GIOVANE ET AL., *supra* note 14, at 23.

doi:10.6342/NTU202402499



them more susceptible to cyberattacks.[180] Additionally, such measures hinder effective fraud detection and prevention by fragmenting data, limiting the effectiveness of fraud detection systems.[181]

b. Cloud Computing Services

Cloud computing services are particularly beneficial to SMEs[182] because they enable users to lease IT resources, including computing power, storage, and database management, through a flexible "pay-as-you-go" pricing model.[183] This allows SMEs to scale up their businesses without requiring significant capital investments.[184]

However, the core principle of the cloud delivery model, "location independence," clearly conflicts with local storage demands.[185] Consequently, local storage requirements may result in several adverse effects, including increased costs for cloud computing services due to limitations on server location flexibility, negative impacts on small businesses' access to digital tools essential for their global expansion, and reduced service availability in certain regions which limit users' choice.[186]

Moreover, compliance costs may escalate due to the complexity of understanding and adhering to diverse local data storage requirements, exacerbated by international regulatory fragmentation.[187] Local storage requirement measures may also raise cybersecurity risks by hindering the mobility of threat data essential for detecting and

[180] *Id.*
[181] *Id.*
[182] *The Transformative Power of Cloud Computing: A Glimpse into the Future,* DIGITAL4BUSINESS (Dec. 14, 2023), https://digital4business.eu/the-benefits-of-cloud-computing-for-smes/ (last visited Apr. 10, 2024).
[183] CHIARA DEL GIOVANE ET AL., *supra* note 14, at 24.
[184] *Id.* at 23.
[185] *Id.*
[186] CHIARA DEL GIOVANE ET AL., *supra* note 14, at 23.
[187] *Id.*

doi:10.6342/NTU202402499

addressing cyber threats globally.[188] Furthermore, there is an increased risk of data loss from natural disasters, undermining the resilience of cloud systems.[189]

D. Local Storage Requirements May Become Barriers to Trade in Services.

As previously noted in Section I, the most prevalent local storage requirements relate to accounting information, financial statements, government data, personal data, and payment-related data. Such local storage requirements can incur compliance costs of establishing or leasing local data servers for foreign entities that possess the aforementioned data. In general, local storage requirements can lead to barriers to trade in services due to the following reasons:

First, local storage requirements may increase costs for foreign service suppliers. For instance, they may need to invest in setting up local data servers or lease server space within the country imposing the requirement. These added expenses can act as a deterrent for foreign service suppliers, making it financially burdensome for them to enter or operate within the market.

Second, complying with local storage requirements may pose technical challenges for foreign service suppliers. They may need to adapt their systems and infrastructure to ensure compliance with the specific storage requirements of each country where they operate. This could involve significant investment in technology and resources, further increasing operational costs and hindering market entry.

Third, local storage requirements may incur a compliance burden. Foreign service suppliers may need to navigate through layers of legal requirements and administrative procedures to ensure compliance. This compliance burden can be particularly challenging

[188] *Id.*
[189] *Id.*

doi:10.6342/NTU202402499

for smaller service suppliers with limited resources and expertise, discouraging them from entering the market or expanding their operations.

In sum, local storage requirements lead to trade barriers in services when the service suppliers do not possess local data servers in every country where they offer their services.

V. SUMMARY

Local storage requirements are one types of data localisation measures, which can be classified into general and sector-specific requirements. General requirements apply to legal and natural entities broadly, while sector-specific ones target particular industries.

Data localisation measures are increasingly common, with nearly 100 measures across 40 countries by early 2023. Nations implement these measures due to various rationales involving data sovereignty, national security, law enforcement, data protection and privacy concerns, geopolitical risks and financial sanctions, and economic protectionism.

Local storage requirements commonly apply to accounting data and financial data, personal information, personal health records and government data. These mandates compel data controllers to store specific data on local data servers or data centers, which can result in substantial compliance costs, technical difficulties, and administrative burdens for foreign entities lacking computing facilities within the regions enforcing these requirements.

Consequently, local storage requirements often create trade barriers for foreign entities that must comply with these mandates. These barriers can affect services when their suppliers are subject to such regulations. To determine whether the trade impact of local storage requirements is regulated within the international trade regime, the

doi:10.6342/NTU202402499

subsequent chapter will assess the consistency of these requirements with the principles outlined in the GATS.

doi:10.6342/NTU202402499

CHAPTER THREE

LOCAL STORAGE REQUIREMENTS AND GATS

GATS is the covered agreement that WTO Members are required to abide by when they impose any measures affecting trade in services.[190] GATS thus provides for rules to prevent certain trade barriers resulting from measures imposed by WTO Members. As previously discussed, local storage requirements can lead to barriers to trade in services, particularly when their suppliers are data controllers who need to comply with the mandates of local data storage.

Accordingly, this chapter explores the compatibility of local storage requirements with GATS. It also discusses the negotiation progress related to data localisation issues under the WTO E-Commerce work program to determine whether these measures have gradually become concerns within the international trade regime.

I. The General Principles and Exceptions of the GATS

Since November 2016, Russia has prohibited access to LinkedIn, a professional networking platform, due to a court ruling asserting its non-compliance with regulations mandating the transfer of Russian user data to servers within the country.[191] This instance illustrates the intricate connection between trade in services and local storage requirements, particularly highlighting the impact on foreign service suppliers whose service operations mainly rely on data gathering and processing.

To deter WTO Members from adopting protectionist measures that create obstacles to trade in services, the multilateral regulations governing trade in services within WTO's

[190] GATS, art. I:1 ("This Agreement applies to measures by Members affecting trade in services.").
[191] Maria Elterman, *Why LinkedIn was banned in Russia,* IAPP (Jan. 23, 2017), https://iapp.org/news/a/why-linkedin-was-banned-in-russia/ (last visited Apr. 11, 2024).

doi:10.6342/NTU202402499

covered agreements are formalized as the GATS. Although there is no explicit prohibition of local storage requirements under the GATS, this section will explore the basic principles thereunder and identify the regulatory constraints surrounding local storage requirements within the context of GATS.

A. Measures Subject to the GATS

Before delving into the general obligations of GATS, it is critical to address whether local storage requirements shall be subject to GATS. GATS Article I:1 offers some insight into this issue.

a. Measures Affecting Trade in Services

GATS Art. I:1 stipulates that GATS applies to measures affecting trade in services. The Appellate Body clarified the concept of a "measure affecting trade in services" in the *Canada — Autos* (2000) case, outlining two key considerations in determining whether a measure falls under this category: (i) whether there is "trade in services" as defined in Article I:2, and (ii) whether the measure "affects" such trade within the meaning of Article I:1.[192]

The Appellate Body in *EC — Bananas III* further clarified that the intention of GATS drafters was to provide a broad scope, as evidenced by the use of the term "affecting."[193] The Panel of *EC–Bananas III* also emphasized that GATS encompasses any measure of a Member to the extent that it impacts the supply of a service, regardless of whether the

[192] Appellate Body Report, *Canada — Certain Measures Affecting the Automotive Industry*, WTO Doc WT/DS139/AB/R (adopted on June 19, 2000), [hereinafter Appellate Body Report, *Canada — Autos (2000)*], ¶ 155; VAN DEN BOSSCHE & ZDOUC, *supra* note 16, at 329.
[193] Appellate Body Report, *European Communities — Regime for the Importation, Sale and Distribution of Bananas*, WTO Doc WT/DS27/AB/R (adopted on Sep. 25, 1997), [hereinafter Appellate Body Report, *EC — Bananas III*], ¶ 220.

doi:10.6342/NTU202402499

measure directly governs the supply of a service or regulates other matters but nevertheless affects trade in services.[194]

b. The Definition of Services

GATS does not provide a specific definition of services.[195] Nonetheless, according to GATS Art.I:3(b), services refer to "any services in any sector except supplied in the exercise of governmental authority." Therefore, only services with a commercial nature are subject to the GATS.

Services also need to be classified in different sectors following the context of GATS. The services sectoral classification list (W/120) is a comprehensive list of services sectors and sub-sectors covered under the GATS, which was compiled by the WTO in July 1991. There are 160 sub-sectors classified thereunder. Although the classification list is not a mandatory classification document, most WTO Members adhere to such a list when making their commitments outlined in the GATS schedule.[196]

c. The Supply of Services

The supply of services refers to the production, distribution, marketing, sale, and delivery of a service pursuant to GATS Article XXVIII(b). Four modes of service supplies are outlined in Article I:2 of the GATS.[197]

---

[194] Panel Report, *European Communities — Regime for the Importation, Sale and Distribution of Bananas*, WTO Doc WT/DS27/R (adopted on Sep. 25, 19970, [hereinafter Panel Report, *EC — Bananas III*], ¶ 7.285.
[195] VAN DEN BOSSCHE & ZDOUC, *supra* note 16, at 329.
[196] TOBIAS NAEF, *supra* note 72, at 243
[197] GATS, art. I:2 ("For the purposes of this Agreement, trade in services is defined as the supply of a service: (a) from the territory of one Member into the territory of any other Member; (b) in the territory of one Member to the service consumer of any other Member; (c) by a service supplier of one Member, through commercial presence in the territory of any other Member; (d) by a service supplier of one Member, through presence of natural persons of a Member in the territory of any other Member."); VAN DEN BOSSCHE & ZDOUC, *supra* note 16, at 329.

doi:10.6342/NTU202402499

Mode 1 of service supplies concerns cross-border service supply, as provided for in Art. I:2(a). Cross-border service supply occurs when any service supplier is located within its own country of one WTO Member and delivers services to any customer residing in different jurisdictions governed by another WTO Member.[198]

Mode 2 of service supplies involves services to be consumed abroad, as outlined in Art. I:2(b). This type of service supplies pertains to situations where any customer seeks services in jurisdictions governed by another WTO Member, and domestic service providers within that jurisdiction supply those services.[199]

Mode 3 of service supplies refers to the commercial presence according to Art. I:2(c). Under this mode, a service supplier establishes a commercial presence within the territory of another WTO Member, from which it offers services to customers located within the same territory.[200]

Mode 4 of service supplies concerns the presence of natural persons, as specified in Art. I:2(d). This mode of supply entails a service supplier physically entering the territory of another WTO Member to provide services to customers residing within that same territory.[201]

d. Local Storage Requirements Affecting Trade in Services of Mode 1 and 2

Although local storage requirements imposed by a WTO Member may not directly restrict trade in services, they inevitably affect services that depend on regular data collection, processing, and transfer. This is particularly notable when service suppliers

[198] VAN DEN BOSSCHE & ZDOUC, *supra* note 16, at 327.
[199] *Id.* at 328.
[200] *Id.* at 328.
[201] *Id.* at 328.

doi:10.6342/NTU202402499

only provide trade in services through Mode 1 and therefore do not have data storage facilities in territories where such requirements are enforced.

For instance, a multinational cloud computing company that offers data storage and processing services globally may be affected by local storage requirements. If a WTO Member enforces a law requiring all personal data of its citizens to be stored locally, the cloud computing company would need to either establish data centres or rent data storage facilities within that Member's border. This may cause significant costs and impact the company's operations, potentially affecting its ability to provide seamless cross-border services. In this scenario, such a requirement is considered a "measure affecting trade in services" and would be subject to GATS.

In addition, local storage requirements could affect Mode 2 of service supplies, given enterprises or natural persons who need to comply with such mandates might seek data storage services within jurisdictions that enforce these requirements.

Nonetheless, a measure affecting trade in services is only inconsistent with GATS when the Member does not abide by the obligations thereunder. To delve deeper into the compatibility of local storage requirements with GATS, the next section outlines the specific GATS obligations that may conflict with these mandates.

B. Most Favoured Nation Treatment and Domestic Regulation Principle

a. GATS Article II:1

GATS Article II:1 prohibits discrimination between services and service suppliers that are like but from different WTO Members.[202] Since local storage requirements generally mandate certain data to be stored within local computing facilities regardless of

[202] GATS, art. II:1.

doi:10.6342/NTU202402499

the origin of data controllers, these requirements typically do not amount to *de jure* discrimination against like foreign service suppliers.

Whether local storage requirements constitute a *de facto* discrimination within the context of GATS Article II:1 depends on whether such requirements modify the conditions of competition between like services and service suppliers from different WTO members.[203]

Therefore, this thesis does not further examine the relationship between local storage requirements and GATS Article II:1, as local storage requirements are typically not inconsistent with GATS Article II:1.

b. GATS Article VI:1

GATS Article VI:1 requests WTO Members to oversee their measures of general application affecting trade in services in sectors where specific commitments are undertaken be administered in a "reasonable, objective and impartial manner."[204] This paragraph aims to prohibit the arbitrary and biased application and administration of domestic regulations and to ensure consistent and predictable administrative decisions.

Therefore, Article VI:1 of the GATS relates to the administration of measures, rather than their substantial content.[205] Accordingly, local storage requirements themselves do not violate GATS Article VI:1, unless the implementation of such requirements is not administered in a "reasonable, objective and impartial manner."

C. Market Access and National Treatment

[203] *See* GATS, art. XVII:3; Appellate Body Report, *Argentina — Measures Relating to Trade in Goods and Services*, WTO Doc WT/DS453/AB/R (adopted on May 9, 2016) [hereinafter Appellate Body Report, *Argentina — Financial Services*], ¶ 6.105.
[204] GATS, art. VI:1.
[205] Appellate Body Report, *EC — Bananas III*, ¶ 200.

doi:10.6342/NTU202402499

Unlike the GATT which applies the national treatment principle and the market access obligation to all WTO Members,[206] the national treatment obligation in GATS Article XVII and the market access obligation in GATS Article XVI only apply to Members who specifically commit to abide by such rules under their GATS schedules. The following subsection briefly introduces the GATS Services Schedule.

a. GATS Services Schedule

GATS regulates trade in services through a positive list approach regarding the application of Articles XVI and XVII. For instance, WTO Members are only obligated to open their markets to foreign services and service suppliers when they commit to market access obligations in their schedule of specific commitments, as required by Article XX:1 of the GATS.[207]

WTO Members often use the Service Sectoral Classification List (W/120) to create their Service schedules.[208] Any modification or withdrawal of commitments by a WTO Member must adhere to the rules outlined in Article XXI GATS, usually involving compensatory adjustments elsewhere.[209] These commitments, detailed in the schedules, are legally binding and integral to the GATS, subject to resolution through WTO dispute settlement mechanisms as specified in Article XXIII:1 GATS.[210]

b. Market Access

[206] GATT, art. XI; art. III.
[207] GATS, art. XX:1 ("Each Member shall set out in a schedule the specific commitments it undertakes under Part III of this Agreement. With respect to sectors where such commitments are undertaken, each Schedule shall specify: (a) terms, limitations and conditions on market access; (b) conditions and qualifications on national treatment; (c) undertakings relating to additional commitments; (d) where appropriate the time-frame for implementation of such commitments; and (e) the date of entry into force of such commitments.").
[208] TOBIAS NAEF, *supra* note 72, at 244.
[209] *Id.*
[210] *See* GATS, art. XXIII:1 ("If any Member should consider that any other Member fails to carry out its obligations or specific commitments under this Agreement, it may with a view to reaching a mutually satisfactory resolution of the matter have recourse to the DSU.").

doi:10.6342/NTU202402499

Market access is one of the common non-tariff barriers to trade in services. For instance, Members may impose regulations to restrict the number of banks within a specific geographical area or the number of foreign lawyers that can practice in their jurisdictions. Although the GATS does not explicitly define what measures can be deemed market access barriers, GATS Article XVI:2(a)-(f) provides an exhaustive list of such measures.[211] This list comprises six types of market access barriers. Five are quantitative restrictions, and the rest concern measures that restrict or require specific types of legal entities or joint ventures through which services may be supplied.

When evaluating the compatibility of local storage requirements with GATS Article XVI:2, subparagraphs (a) and (c) are most frequently examined.[212] GATS Article XVI:2(a) prohibits limitations on the number of service suppliers, while Article XVI:2(c) prohibits limitations on the number of service operations.

The definition of the supply of services under GATS Article XXVIII(b) encompasses a wide range of activities, including the production, distribution, marketing, sale, and delivery of services.[213] When data storage is integral to the said services, local storage requirements may become restrictions on the supply of services.

---

[211] GATS, art. XVI:2 ("In sectors where market-access commitments are undertaken, the measures which a Member shall not maintain or adopt either on the basis of a regional subdivision or on the basis of its entire territory, unless otherwise specified in its Schedule, are defined as: (a) limitations on the number of service suppliers whether in the form of numerical quotas, monopolies, exclusive service suppliers or the requirements of an economic needs test; (b) limitations on the total value of service transactions or assets in the form of numerical quotas or the requirement of an economic needs test; (c) limitations on the total number of service operations or on the total quantity of service output expressed in terms of designated numerical units in the form of quotas or the requirement of an economic needs test; (d) limitations on the total number of natural persons that may be employed in a particular service sector or that a service supplier may employ and who are necessary for, and directly related to, the supply of a specific service in the form of numerical quotas or the requirement of an economic needs test; (e) measures which restrict or require specific types of legal entity or joint venture through which a service supplier may supply a service; and (f) limitations on the participation of foreign capital in terms of maximum percentage limit on foreign share-holding or the total value of individual or aggregate foreign investment.").

[212] TOBIAS NAEF, *supra* note 72, at 308; *The Data Localization Debate in International Trade Law*, IKIGAI LAW (June 22, 2020), https://www.ikigailaw.com/the-data-localization-debate-in-international-trade-law/#_ftn17.

[213] GATS, art. XXVIII(b) ("supply of a service" includes the production, distribution, marketing, sale and

doi:10.6342/NTU202402499

Naef suggests that local storage requirements may cause market access restrictions to the cross-border supply of services, i.e., Mode 1 supply of services.[214] Firstly, the Scheduling Guidelines of 2001 clarify that under mode 1 of service supply, the service supplier is not physically present within the Member's territory where the service is delivered.[215]

In addition, when WTO Members commit fully to Mode 1, Crosby asserts that "it may not condition the supply of cross-border services on the service suppliers' presence or operation within its territory."[216] While local storage requirements may not explicitly mandate the local presence or commercial presence of service suppliers, the necessity of storing data locally inherently requires service suppliers to operate data storage facilities within the territory. Thus, Naef argues that requirement contradicts the fundamental concept of cross-border service supply.[217]

Specifically, local storage requirements may constitute limitations to the number of service suppliers and service operations under GATS Article XVI(a) and (c) and therefore constitute market access restrictions. GATS Article XVI:2(a) and (c) prohibit quantitative restrictions on market access.[218] The Appellate Body has elaborated measures completely prohibiting service supply amount to a market access limitation under Article XVI:2(a) and (c) because they reduce the number of service suppliers, operations, and output to zero.[219]

---

delivery of a service").
[214] TOBIAS NAEF, *supra* note 72, at 309.
[215]Council on Trade in Services, *Guidelines for the Scheduling of Specific Commitments und the General Agreement on Trade in Services* (GATS), WTO Doc S/L/92 (March 28, 2001), ¶ 28.
[216] Daniel Crosby, *Analysis of Data Localization Measures Under WTO Services Trade Rules and Commitments*, INTERNATIONAL CENTER FOR TRADE AND SUSTAINABLE DEVELOPMENT & WORLD ECONOMIC FORUM E15INITIATIVE (2016), http://e15initiative.org/wpcontent/uploads/2015/09/E15-Policy-Brief-Crosby-Final.pdf, at 3.
[217] TOBIAS NAEF, *supra* note 72, at 309.
[218] *Id.*
[219] Appellate Body Report, *United States — Measures Affecting the Cross-Border Supply of Gambling and*

doi:10.6342/NTU202402499

Naef argues that local storage requirements effectively lead to a zero quota for cross-border service suppliers and operations.[220] This essentially prohibits mode 1 service supply and service suppliers, which do not need any physical presence within a Member's territory.[221] Consequently, local storage requirements may conflict with the market access obligations outlined in GATS Article XVI:2(a) and (c).

To date, the WTO jurisprudence has not clarified in any case whether local storage requirements amount to violations of GATS Article XVI:2(a) and (c). This thesis agrees that local storage requirements may impose additional compliance costs for cross-border service suppliers who lack local storage facilities. However, it is debatable whether these rules require the physical presence of cross-border service suppliers. For instance, service suppliers can lease local computing facilities to comply with such mandates without establishing any commercial presence or service operations. In this scenario, service suppliers can still operate from outside the territories where local storage requirements are enforced.

In conclusion, although some scholars assert that local storage requirements contradict the cross-border supply of services, this thesis contends that while these requirements may increase compliance costs, they may not prohibit cross-border service operations and service suppliers. Hence, local storage requirements do not necessarily become inconsistent with GATS Article XVI:2(a) and (c).

c. National Treatment Obligation

Betting Services, WTO Doc WT/DS285/AB/R (adopted on April 20, 2005), [hereinafter Appellate Body Report, *US — Gambling*], ¶¶ 232; 252.

[220] TOBIAS NAEF, *supra* note 72, at 309.

[221] *Id.*

doi:10.6342/NTU202402499

GATS Article XVII paragraph 1 provides for national treatment obligation, which requires WTO Members to provide treatment no less favourable than it accords to its own like services and service suppliers.

Unlike GATT Article III, which imposes a national treatment obligation on WTO Members as a general principle, GATS Article XVII applies only when a WTO Member has explicitly committed to providing national treatment for the specific services sector in their Schedule of Specific Commitments.[222]

To determine if a measure is inconsistent with GATS Article XVII:1, the WTO Panel applies a four-tier test to examine (i) whether a Member has committed to a national treatment obligation for the relevant services sector and mode of supply; (ii) whether the measure at issue affects trade in services (iii) the likeness between foreign and domestic services and service suppliers and (iv) the measure treats foreign like services and service suppliers less favourable than their domestic counterparts.[223]

i. National Treatment Commitment

National treatment commitments are outlined in a Member's "Schedule of Specific Commitments" and often come with conditions, qualifications, and limitations.[224] WTO Members are entitled to grant national treatment for a specific service sector only for certain modes of supply but exclude others.[225] Therefore, when a Member does not commit to undertaking the national treatment obligation for certain modes of supply in a

[222] VAN DEN BOSSCHE & ZDOUC, *supra* note 16, at 400.
[223] Panel Reports, *EC — Bananas III (1997)*, WT/DS27/R (adopted on May 22, 1997), [hereinafter Panel Reports, *EC — Bananas III (1997)*], ¶ 7.314.
[224] VAN DEN BOSSCHE & ZDOUC, *supra* note 16, at 400.
[225] *Id.*

doi:10.6342/NTU202402499

specific sector, local storage requirements are not subject to GATS Article XVII:1 even if they affect those services or service suppliers in that specific sector and mode of supply.

For instance, the Russian Federation does not commit to undertaking the national treatment obligation for mode one of supply in services incidental to energy distribution, which only concerns consulting services.[226] Accordingly, even if local storage requirements incur extra compliance costs for cross-border like service suppliers in this sector, they are not subject to GATS Article XVII:1 due to the absence of a national treatment commitment for mode one supply.

ii. Like Services and Service Suppliers

GATS Article XVII:1 only applies to measures that accord less favourable treatment to like foreign services and service suppliers. In terms of the "likeness" criteria, the Appellate Body in *Argentina — Financial Services (2016)* clarified that it involves the consideration of three factors: (1) characteristics of services and service suppliers, (2) consumers' preferences regarding services and service suppliers, and (3) tariff classification and description of services, such as those found in the UN Central Product Classification (CPC).[227] However, it is worth noting that these criteria are merely analytical tools to examine likeness rather than mandatory elements.[228]

To determine the essential similarity required for services to be considered "like", the Panel in *China — Electronic Payment Services (2012)* referred to Article XVII:3 of the GATS, which clarifies the requirement of providing treatment no less favorable.[229] This

[226] Russian Federation Schedule of Specific Commitments, Trade in Services, WTO Doc GATS/SC/149, Nov. 5, 2012, at 21.
[227] Appellate Body Report, *Argentina — Financial Services*, ¶ 6.32.
[228] *Id.*
[229] Panel Report, *China — Certain Measures Affecting Electronic Payment Services,* WTO Doc WT/DS413/R (adopted on Aug. 31, 2012) [hereinafter Appellate Body Report, *China — Electronic Payment Services*], ¶ 7.699.

doi:10.6342/NTU202402499

article states that less favorable treatment occurs if a WTO Member modifies competition conditions in favour of its own services compared to those of other Members. Consequently, the Panel concluded that "like services" are those in a competitive relationship with each other because only services in such relationships can be affected by measures that favour one over the other.[230]

As previously introduced, local storage requirements can be classified into general and sector-specific requirements. For instance, a general requirement may request that personal data be stored locally. In this case, any service suppliers possessing personal data shall comply with this requirement, and thus whether services and services suppliers affected thereby are "like" depends on case-by-case analysis.

Sector-specific requirements typically affect like services and service suppliers. To elaborate, a government mandate requiring the health services sector to store health data locally could affect both domestic and foreign like health services and service suppliers.

iii. Treatment No Less Favourable

Local storage requirements are inconsistent with GATS Article XVII:1 when they not only affect like foreign services and service suppliers in the modes of supply where a Member has undertaken a national treatment commitment, but also when they accord less favorable treatment to these like foreign services and service suppliers.

Paragraphs 2 and 3 of Article XVII clarify that a Member may provide either formally identical or different treatment to foreign services and service suppliers compared to domestic counterparts; However, such treatment is considered less favourable if it

[230] *Id*. ¶ 7.700.

doi:10.6342/NTU202402499

modifies the conditions of competition in favour of services or service suppliers of the Member compared to like services or service suppliers of any other Member.

Thus, even if a Member offers formally identical treatment to both foreign and domestic like services and services suppliers, it could still violate the national treatment obligation if it modifies the conditions of competition in favour of the domestic services or service suppliers.[231]

Nonetheless, it is important to note that any inherent competitive disadvantage arising from the foreign nature of services or service suppliers cannot be deemed *de facto* discrimination against foreign like services and service suppliers.[232] In *Argentina — Financial Services (2016)*, the Appellate Body asserts that "inherent competitive disadvantages" must be intrinsic to the foreign nature of the services and suppliers, rather than being caused by the measure affecting trade in services.[233]

Local storage requirements typically apply to data controllers possessing certain data regardless of their nationality, thus offering formally identical treatment to foreign and domestic like services and service suppliers. Hence, whether a local storage requirement is inconsistent with GATS Article XVII:1 depends on whether this requirement *de facto* imposes an extra burden on foreign like services and service suppliers in favour of domestic services or service suppliers.

iv. The Relationship Between Local Storage Requirement and GATS Article XVII:1

[231] VAN DEN BOSSCHE & ZDOUC, *supra* note 16, at 409.
[232] GATS, art. XVII, footnote 10 ("Specific commitments assumed under this Article shall not be construed to require any Member to compensate for any inherent competitive disadvantages which result from the foreign character of the relevant services or service suppliers").
[233] Appellate Body Report, *Argentina — Financial Services*, ¶ 6.146.

doi:10.6342/NTU202402499

GATS Article XVII:1 may be one of the most relevant GATS provisions that is incompatible with local storage requirements. However, members are only obligated to comply with GATS Article XVII:1 when they have made a national treatment commitment for specific modes of supply in designated service sectors. Therefore, if local storage requirements accord less favorable treatment to particular modes of supply of certain foreign like services or service suppliers without such commitments, Article XVII:1 does not impose any obligations on members enforcing these requirements.

Additionally, determining whether local storage requirements accord less favorable treatment to foreign like services and service suppliers necessitates a case-by-case analysis. Local storage requirements mandate data controllers to store data within a specific geographical region. Consequently, service suppliers required to comply with these mandates but lacking local storage facilities in the region may incur compliance costs associated with establishing or leasing such facilities.

Nonetheless, due to the trend of cloud storage,[234] both domestic and foreign service suppliers can bear compliance costs if they lack data storage facilities in regions where local storage requirements are enforced. Accordingly, even if these requirements impose financial burden on data controllers, it remains debatable whether they modify the competitive relationship between domestic and foreign like service suppliers when both use cloud storage and lack local storage facilities,

Moreover, when foreign service suppliers face the additional burden of leasing or establishing local storage facilities, it raises the question of whether such burdens are inherent competitive disadvantages stemming from their foreign nature. As previously

[234] Aron Wagner, *The Future of Cloud Storage: Trends and Predictions, American Cloud* (Dec. 5, 2023), AMERICAN CLOUD, https://americancloud.com/blog/the-future-of-cloud-storage-trends-and-predictions (last visited at July 7, 2024).

doi:10.6342/NTU202402499

mentioned, "inherent competitive disadvantages" are those intrinsic to the foreign nature of the service suppliers rather than being caused by the measure at issue.[235] Local storage requirements do not mandate investments in building or leasing local storage facilities. However, cross-border foreign service suppliers may inevitably need to invest in such facilities if they do not have them locally. One could argue that these competitive disadvantages are intrinsic to their foreign nature rather than being a direct result of local storage requirements.

In sum, local storage requirements are not necessarily inconsistent with GATS Article XVII:1. In addition, this article does not prevent local storage requirements from affecting services and service suppliers when members have not made national treatment commitments.

D. General and Security Exceptions of the GATS

GATS is designed to promote the liberalization of trade in services while also acknowledging and safeguarding the ability of governments to pursue essential national objectives, such as public health, environmental protection, and national security.[236] Trade liberalization often leads to the availability of better and cheaper products and services, which can facilitate societal values and interests.[237] However, when pursuing legitimate societal interests, governments also enact legislation or measures that may inadvertently create trade barriers,[238] conflicting with GATS rules on non-discrimination and market access.

[235] Appellate Body Report, *Argentina — Financial Services*, ¶ 6.146.

[236] VAN DEN BOSSCHE & ZDOUC, *supra* note 16, at 544.
[237] *Id.* at 545.
[238] *Id.*

doi:10.6342/NTU202402499

Accordingly, GATS seeks to reconcile trade liberalization with the need to protect and promote other societal values and interests, providing checks and balances to address political and economic concerns. Therefore, GATS also provides for exceptions for Members to deviate from their obligations thereunder. This section introduces both the general exceptions and security exceptions under the GATS.

a. Article XIV of the GATS

GATS Article XIV provides the following:

> Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures:
>
> (a) necessary to protect public morals or to maintain public order;
>
> (b) necessary to protect human, animal or plant life or health;
>
> (c)necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to:
>
> (i) the prevention of deceptive and fraudulent practices or to deal with the effects of a default on services contracts;
>
> (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;
>
> (iii) safety;

doi:10.6342/NTU202402499

(d) inconsistent with Article XVII, provided that the difference in treatment is aimed at ensuring the equitable or effective imposition or collection of direct taxes in respect of services or service suppliers of other Members;

(e) inconsistent with Article II, provided that the difference in treatment is the result of an agreement on the avoidance of double taxation or provisions on the avoidance of double taxation in any other international agreement or arrangement by which the Member is bound.

The comparison between GATT Article XX and GATS Article XIV reveals notable similarities and differences. While both articles provide exceptions to trade obligations, certain justifications present in GATS Article XIV, such as maintaining public order and protecting safety and privacy, are absent in GATT Article XX. [239] Conversely, some exceptions in GATT Article XX, such as protecting national treasures, do not appear in GATS Article XIV. [240]

Despite these differences, the architectural and conceptual resemblance between the two articles enables the interpretation of GATS Article XIV using precedents set by GATT Article XX. [241] The Appellate Body's ruling in the *US — Gambling* case confirmed that past decisions regarding GATT Article XX are considered relevant for interpreting Article XIV of the GATS.[242]

GATS Article XIV establishes a two-tier test similar to GATT Article XX for justifying measures that may otherwise be inconsistent with GATS obligations. This test involves first determining if the challenged measure falls within the scope of one of the

[239] VAN DEN BOSSCHE & ZDOUC, *supra* note 16, at 606.
[240] *Id.*
[241] *Id.*
[242] Appellate Body Report, *US — Gambling*, ¶ 291.

doi:10.6342/NTU202402499

paragraphs of GATS Article XIV, addresses a specific interest, and has a sufficient connection to the protected interest. If so, the measure must then satisfy the requirements of the chapeau of GATS Article XIV.[243] Thus, the justification under Article XIV of the GATS involves assessing both the measure's alignment with specific paragraphs concerning the pursuit of societal values other than trade liberalization and its compliance with the chapeau of the GATS.

As previously introduced in Chapter II, the rationales behind local storage requirements include the pursuit of national security, personal privacy, and law enforcement. These mandates may be relevant to achieve the national objectives outlined in GATS Article XIV(a) or (c). Consequently, this subsection examines the specific paragraphs outlined in GATS Article XIV(a) and (c) and evaluates the criteria outlined in the chapeau of GATS Article XIV.

i. GATS Article XIV(a)

Article XIV(a) of the GATS addresses measures deemed necessary to safeguard public morals or uphold public order and establishes a two-tier legal standard for determining their provisional justification.[244] To invoke GATS Article XIV(a), a Member must demonstrate that the measure is aimed at protecting public morals or maintaining public order and that it is necessary to achieve that policy goal.[245]

The interpretation of "public morals" and "public order" may vary based on cultural, social, and religious factors, with Members having the autonomy to determine the appropriate level of protection.[246] The Panel in the *US — Gambling* case highlighted the

[243] *Id.* at 607.
[244] VAN DEN BOSSCHE & ZDOUC, *supra* note 16, at 608.
[245] *Id.*
[246] *Id.*

doi:10.6342/NTU202402499

importance of allowing Members to define and apply these concepts within their own territories based on their respective systems and values.[247]

Furthermore, "public morals" and "public order" in GATS Article XIV(a) need to be interpreted in the context of protecting societal interests. The Panel in the *US — Gambling* case determined that "public morals" refers to standards of right and wrong conduct maintained by a community or nation,[248] while "public order" relates to preserving fundamental societal interests such as law, security, and morality.[249] The Panel acknowledged the overlap between these concepts to the extent that they largely protect similar values.[250]

Regarding the necessity requirement of GATS Article XIV(a), in *US — Gambling*, the Panel and Appellate Body considered the importance of the interests at stake and the restrictive impact of the measure at issue on international commerce.[251] They also emphasized the need to weigh and balance the contribution of the measure to its objectives against its impact on commerce.[252] The burden of proof lies with the responding party to demonstrate the necessity of the measure, but they are not required to identify all theoretically possible reasonably available alternative measures.[253] Instead, only when the complaining party presents a less trade restrictive alternative that is reasonably available would the burden shifts to the responding party to justify the necessity of their measure in comparison to the proposed alternative.[254]

---

[247] Panel Report, *United States — Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WTO Doc WT/DS285/R (adopted on Apr. 20, 2005) [hereinafter Panel Report, *US — Gambling*], ¶ 6.461.
[248] Panel Report, *US — Gambling*, ¶ 6.465.
[249] Panel Report, *US — Gambling*, ¶ 6.467.
[250] Panel Report, *US — Gambling*, ¶ 6.468.
[251] Appellate Body Report, *US — Gambling,* ¶ 306.
[252] *Id.*
[253] Appellate Body Report, *US — Gambling,* ¶ 309-11.
[254] *Id.*

doi:10.6342/NTU202402499

The Panel in *US — Gambling* found that the US had not proven the "necessity" of its measures because it failed to explore available WTO-consistent alternatives, such as bilateral or multilateral consultations with Antigua.[255] The Appellate Body disagreed with this assessment, stating that consultations were not a "reasonably available" alternative to the U.S.[256] Upon review, the Appellate Body determined that the measures, including laws prohibiting internet gambling, were indeed necessary for maintaining public order and protecting public morals under GATS Article XIV(a) because the US had demonstrated the prima facie case of "necessity" and Antigua had not proposed any "reasonably available" alternatives. Therefore, the measures were justified under GATS Article XIV(a).[257]

ii. GATS Article XIV(c)

GATS Article XIV(c) provides a basis for justifying measures that would otherwise conflict with GATS obligations if these measures are deemed necessary to secure compliance with laws or regulations that are not inconsistent with the provisions of the GATS. Specifically, GATS Article XIV(c) outlines three main categories of such laws or regulations: (i) those concerning the prevention of deceptive practices or defaults on service contracts, (ii) laws concerning the protection of individual privacy regarding personal data processing and dissemination, and safeguarding confidentiality of personal records and accounts, and (iii) laws concerning the safety.

However, as observed by the Panels in *US — Gambling* and *Argentina - Financial Services*, this list is not exhaustive,[258] and GATS Article XIV(c) extends to other types of

[255] Panel Report, *US — Gambling*, ¶ 6.531.
[256] Appellate Body Report, *US — Gambling,* ¶ 317.
[257] Appellate Body Report, *US — Gambling,* ¶ 326.
[258] Panel Report, *US — Gambling*, ¶ 6.540; Panel Report, *Argentina — Measures Relating to Trade in Goods and Services*, WTO Doc WT/DS453/R (adopted on May 9, 2016), [hereinafter Panel Report, *Argentina — Financial Services*], ¶ 7.583.

doi:10.6342/NTU202402499

laws or regulations not explicitly mentioned, akin to the scope provided by GATT Article XX(d). Consequently, GATS Article XIV(c) allows for the pursuit of various policy objectives beyond those specifically stated.[259]

In *Argentina — Financial Services*, the Appellate Body clarified the requirements of GATS Article XIV(c), focusing on two key elements: the assessment of the measure's design and its necessity.[260] The measure must be designed to secure compliance with specific laws or regulations even if absolute certainty of compliance cannot be guaranteed.[261] However, if it is evident that the measure cannot achieve compliance, further analysis of its necessity may not be necessary.[262] The Appellate Body emphasized that a measure not designed to ensure compliance cannot be justified under Article XIV(c).[263]

The process of determining the necessity of a measure under GATS Article XIV(c) mirrors the examination required under GATS Article XIV(a), as discussed previously. As outlined in *US — Gambling*, the assessment begins with evaluating the relative importance of the interests or values promoted by the measure.[264] Subsequently, the panel considers additional factors such as the measure's contribution to achieving its objectives and its impact on international commerce.[265] A comparison between the challenged measure and possible alternatives is then conducted, with the results weighed against the significance of the interests at stake. Based on this comprehensive analysis, whether the

[259] VAN DEN BOSSCHE & ZDOUC, *supra* note 16, at 612.
[260] Appellate Body Report, *Argentina — Financial Services*, ¶ 6.202.
[261] Appellate Body Report, *Argentina — Financial Services*, ¶ 6.203.
[262] *Id.*
[263] *Id.*
[264] Appellate Body Report, *US — Gambling,* ¶ 306-7.
[265] *Id.*

doi:10.6342/NTU202402499

measure is necessary or if there exists another WTO-consistent measure that is reasonably available will be determined.[266]

iii. Chapeau of GATS Article XIV

The chapeau of the GATS prohibits (i) arbitrary or unjustifiable discrimination between countries where like conditions prevail and (ii) disguised restrictions on trade in services. The language of GATS Article XIV chapeau closely resembles that of GATT Article XX. Therefore, the examination standards from extensive GATT Article XX jurisprudence can be applied to GATS Article XIV.[267]

1. Arbitrary or Unjustifiable Discrimination

In the *US — Shrimp*, the Appellate Body identified three conditions necessary to establish "arbitrary or unjustifiable discrimination": (1) the measure in question must lead to discrimination in its application; (2) this discrimination must be characterized by arbitrariness or lack of justification; and (3) this discrimination must occur between countries where the same conditions prevail.[268]

In the *US — Shrimp*, the Appellate Body determined that the implementation of the measure in question constituted "arbitrary discrimination."[269] This conclusion was reached because the measure required countries seeking certification to adopt a regulatory program identical to that of the US without considering its suitability for the exporting

[266] *Id.*
[267] VAN DEN BOSSCHE & ZDOUC, *supra* note 16, at 616.
[268] Appellate Body Report, *United States — Import Prohibition of Certain Shrimp and Shrimp Products*, WTO Doc WT/DS58/AB/R (adopted on November 6, 1998), [hereinafter Appellate Body Report, *US — Shrimp (1998)*], ¶ 150.
[269] Appellate Body Report, *US — Shrimp (1998)*, ¶ 177.

doi:10.6342/NTU202402499

countries' conditions.[270] Additionally, officials lacked flexibility in the certification process, further contributing to the perception of "arbitrary discrimination."[271]

In the *US — Gasoline* case, the Appellate Body determined that the measure in question amounted to "unjustifiable discrimination." This conclusion was based on two key omissions by the US: (i) the failure to adequately explore means, including cooperation with Venezuela and Brazil, to mitigate administrative problems cited as justification for rejecting individual baselines for foreign refiners, and (ii) the failure to consider the costs for foreign refiners resulting from the imposition of statutory baselines. These omissions were deemed excessive for establishing a violation of GATT Article III:4, indicating that the resulting discrimination was foreseeable rather than inadvertent or unavoidable. As a result, the baseline establishment rules in the Gasoline Rule were found to constitute "unjustifiable discrimination" in their application.[272]

In *US — Shrimp*, the Appellate Body also examined whether the implementation of the measure in question constituted "unjustifiable discrimination" within the chapeau's scope.[273] It noted that the US failed to engage in comprehensive negotiations with shrimp-exporting Members regarding sea turtle protection before enforcing the import prohibition.[274] Despite the US' recognition of the importance of international agreements for sea turtle conservation, they only engaged with some Members for negotiations, not all, leading to discriminatory treatment.[275] Consequently, the Appellate Body concluded

[270] *Id.*
[271] *Id.*
[272] Appellate Body Report, *United States — Standards for Reformulated and Conventional Gasoline*, WTO Doc WT/DS2/AB/R (adopted on May 20, 1996), [hereinafter Appellate Body Report, *US — Gasoline (1996)*], at 28–29.
[273] Appellate Body Report, *US — Shrimp (1998)*, ¶ 166.
[274] *Id.*
[275] Appellate Body Report, *US — Shrimp (1998)*, ¶ 172.

doi:10.6342/NTU202402499

that the US's discriminatory actions were unjustifiable, especially considering the lack of effort to establish consensual means of protection for marine resources.[276]

It is worth noting that the language used in the chapeau of GATS Article XIV refers to "arbitrary or unjustifiable discrimination between countries where "like" conditions prevail." On the other hand, the chapeau of Article XX of the GATT 1994 uses the language of "countries where the same conditions prevail." Therefore, Article XIV of the GATS provides for a stricter requirement than that of GATT 1994.[277]

With regard to the element of "where the same conditions prevail between countries," in *US — Shrimp (1998)*, the Appellate Body clarified that arbitrary or unjustifiable discrimination can occur not only between exporting Members but also between exporting Members and the importing Member.[278] In *EC — Seal Products (2014)*, the Appellate Body emphasized that the relevant "conditions" should be determined by the subparagraph of Article XX under which the measure was provisionally justified and the substantive obligations of the GATT.[279] It further stated that respondents who claim that conditions in different countries are not the same must bear the burden of proofs, otherwise the conditions were assumed to be the same.[280]

2. Disguised Restriction on International Trade

In *US — Gasoline*, the Appellate Body discussed the requirement that the application of a measure should not be a "disguised restriction on international trade." [281] They

[276] *Id.*
[277] VAN DEN BOSSCHE & ZDOUC, *supra* note 16, at 616.
[278] Appellate Body Report, *US — Shrimp (1998)*, ¶ 150.
[279] Appellate Body Report, *European Communities — Measures Prohibiting the Importation and Marketing of Seal Products*, WTO Doc WT/DS401/AB/R (adopted on June 18, 1997), [hereinafter Appellate Body Reports, *EC — Seal Products (2014)*], ¶ 5.301.
[280] Appellate Body Reports, *EC — Seal Products (2014)*, ¶ 5.317.
[281] Appellate Body Report, *US — Gasoline (1996)*, at 25.

doi:10.6342/NTU202402499

explained that terms like "arbitrary discrimination," "unjustifiable discrimination," and "disguised restriction" are interconnected and provide context to each other.[282]

The Appellate Body emphasized that restrictions amounting to arbitrary or unjustifiable discrimination under the guise of a measure falling within an exception listed in Article XX can be considered a "disguised restriction."[283] They further noted that the considerations relevant to determining whether a measure constitutes arbitrary or unjustifiable discrimination could also apply to assessing whether it constitutes a disguised restriction on trade.[284] Overall, the objective is to prevent abuse or improper use of exceptions to substantive trade rules outlined in GATT Article XX.[285]

In *EC — Asbestos*, the Panel clarified the requirement of the chapeau regarding the prohibition of a "disguised restriction on international trade."[286] They explained that the term "disguised" is crucial in understanding what falls under this provision.[287] According to the Vienna Convention, "to disguise" implies intention, suggesting actions like concealing, altering to deceive, misrepresenting, or dissimulating.[288] Therefore, a restriction that appears to meet the conditions of Article XX(b) but is actually a disguise to conceal trade-restrictive objectives constitutes an abuse of the provision.[289]

b. Article XIV *bis* of the GATS

[282] *Id.*
[283] *Id.*
[284] *Id.*
[285] *Id.*
[286] Panel Report, *European Communities — Measures Affecting Asbestos and Products Containing Asbestos*, WTO Doc WT/DS135/R (adopted on April 5, 2001), [hereinafter Panel Report, *EC — Asbestos (2001)*], ¶ 8.236.
[287] *Id.*
[288] *Id.*
[289] *Id.*

doi:10.6342/NTU202402499

Article XIV *bis* of the GATS provides for security exceptions to justify measures that are inconsistent with the GATS. It provides the following:

> 1. Nothing in this Agreement shall be construed:
>
> (a) to require any Member to furnish any information, the disclosure of which it considers contrary to its essential security interests; or
>
> (b) to prevent any Member from taking any action which it considers necessary for the protection of its essential security interests:
>
> (i) relating to the supply of services as carried out directly or indirectly for the purpose of provisioning a military establishment;
>
> (ii) relating to fissionable and fusionable materials or the materials from which they are derived;
>
> (iii) taken in time of war or other emergency in international relations; or
>
> (c) to prevent any Member from taking any action in pursuance of its obligations under the United Nations Charter for the maintenance of international peace and security.
>
> 2. The Council for Trade in Services shall be informed to the fullest extent possible of measures taken under paragraphs 1(b) and (c) and of their termination.

The wording of GATS Article XIV *bis* closely resembles that of Article XXI of the GATT 1994.[290] Therefore, the case law concerning GATT Article XXI may be referred

[290] VAN DEN BOSSCHE & ZDOUC, *supra* note 16, at 623.

doi:10.6342/NTU202402499

to when examining whether a measure may invoke GATS Article XIV *bis*.[291] This section reviews how previous WTO cases have addressed the invocation of GATT Article XXI as to provide insights into how GATS Article XIV *bis* can be used as a justification for Members deviating from their obligations.

i. The Debate of "Self-Judging" Nature

GATT Article XXI has been commonly understood as "self-judging" due to the phrase "action which it considers necessary" in its wording.[292] One view suggests that a Member can independently determine if a measure is essential to its security interests and aligns with the subparagraphs of GATT Article XXI.[293] Another perspective acknowledges a Member's right to decide on the applicability of a security exception but requires this decision to meet a good faith standard being subject to judicial review.[294] The third interpretation allows a Member to decide if it deems a measure necessary for protecting its essential security interests, while the specified conditions of GATT Article XXI(a), (b), and (c) are open to judicial review.[295]

In the *Russia — Traffic in Transit* case, the Panel issued its first ruling on the nature of the GATT national security exception.[296] The Panel claimed that GATT Article XXI(b)(iii) is not completely "self-judging" and acknowledged its justiciability.[297] In addition, the Panel leaned towards the third interpretation,[298] asserting that the subparagraphs of GATT Article XXI shall be subject to review by the WTO adjudicative

[291] *Id.*
[292] *See* Roger P. Alford, *The Self-Judging WTO Security Exception*, 3 UTAH L. REV. 697 (2011), at 702.
[293] *Id.* at 704.
[294] *Id.*
[295] *Id.*
[296] Panel Report, *Russia — Measures Concerning Traffic in Transit,* WTO Doc WT/ DS512/ R (adopted on Apr. 26, 2019), [hereinafter Panel Report, *Russia — Traffic in Transit*], ¶ 7.5-7.5.7.
[297] *Id.* ¶ 7.58.
[298] *Id.* ¶ 7.102.

doi:10.6342/NTU202402499

body based on objective determinations.[299] Therefore, for any measure to fall under GATT Article XXI(b), it must objectively meet the requirements outlined in one of its subparagraphs.[300]

ii. The Extent of "Self-Judging"

Another important issue addressed by the Panel in *Russia — Traffic in Transit* is whether the "self-judging" discretion applies solely to the "necessity" of the measure at issue or both the "necessity" and the "essential security interest" under GATT Article XXI(b)(iii).[301]

According to the Panel, each Member has the discretion to define its "essential security interests" following the good faith principle outlined in Article 31(1) of the Vienna Convention on the Law of Treaties,[302] ensuring the security exception is not used to circumvent GATT obligations.[303]

In addition, Members must also establish a good faith connection between the measures and the essential security interests they aim to protect, demonstrating that the measures are not implausible in serving their stated purpose.[304]

Lastly, the determination of whether specific measures are "necessary" for protecting essential security interests is left to the Member with no requirement for proportionality.[305]

II. Case Study: Russian Federal Law No. 242-FZ

[299] *Id.*
[300] Panel Report, *Russia — Traffic in Transit*, ¶ 7.101.
[301] *Id.* ¶ 7.127.
[302] *Id.* ¶ 7.132.
[303] *Id.* ¶ 7.133.
[304] *Id.* ¶ 7.138.
[305] *Id.* ¶ 7.147.

doi:10.6342/NTU202402499

Russian Federal Law No. 242-FZ (hereinafter "No. 242-FZ"),[306] was implemented to amend Federal Law No. 152-FZ, the Procedure for Personal Data Processing in Information-Telecommunication Networks (hereinafter "PDPL").[307]

Article 18:5 of the PDPL mandates:

> when collecting personal data, including through the information and telecommunications network the Internet, the controller is obliged to ensure the recording, arrangement, accumulation, storage, rectification (updating, changing), and extraction of personal data of citizens of the Russian Federation using databases located within the territory of the Russian Federation, with the exception of the cases specified in clauses 2, 3, 4, 8 of part 1 of article 6 of this Federal Law.[308]

Accordingly, any data controller who collects personal data concerning Russian nationals must store that data in servers physically located in Russia. Non-compliance with data protection regulations may result in the blocking of the website utilized for data processing, as exemplified by the ban on LinkedIn.[309]

LinkedIn is a widely popular professional networking platform founded in 2003, which serves as a hub for connecting with others, exploring job opportunities, and advancing careers. With over 810 million active users across 200 countries, LinkedIn has

[306] Russian Federation Federal Law on Personal Data, 2014 (No. 242-FZ).
[307] *Russian Federation Federal Law on Personal Data*, ONE TRUST DATA GUIDANCE, https://www.dataguidance.com/sites/default/files/en_20190809_russian_personal_data_federal_law_2.pd.
[308] *Id.*
[309] Helena Ursic ET AL., *supra* note 40, at 17.

doi:10.6342/NTU202402499

become one of the premier online professional networks globally.[310] In October 2016, there were 3.5 million Russian users of LinkedIn.[311] Nonetheless, LinkedIn failed to present evidence of storing Russian citizen's data in Russia, prompting the Russian Federal Service for Supervision of Communications("Roskomnadzor") to initiate legal action against LinkedIn in a Russian court.[312]

In August 2016, a Moscow court declared that LinkedIn should be banned in Russia due to its practice of storing Russian citizens' data outside the country, which contravened the newly enacted data retention law, Federal Law No. 242-FZ.[313] This ruling was subsequently upheld on November 10, 2016. The official ban, enforced by the Russian Federal Service for Supervision of Communications ("Roskomnadzor"), Information Technology and Mass Media, took effect on November 17, 2016.[314]

On 17 November 2016, Roskomnadzor started to forbid LinkedIn to continue supplying any services to Russian citizens, including blocking the website of LinkedIn and its mobile applications on the territory of the Russian Federation and requesting Apple and Google to remove Russian versions of LinkedIn's online applications from App Store and Google Play online shops.[315] On July 1, 2014, LinkedIn is still forbidden to provide services to Russian citizens within Russia unless they use a foreign VPN to get

[310] Lauren Mak & Chris Bluvshtein, *How to Unblock LinkedIn From Russia in 2024: A Full Guide*, VPNOVERVIEW (Mar. 18, 2024), https://vpnoverview.com/unblocking/censorship/access-linkedin-russia/#:~:text=Is%20LinkedIn%20allowed%20in%20Russia,Russia%20in%20a%20few%20steps (last visited Apr. 10, 2024).
[311] *Id.*
[312] Helena Ursic ET AL., *supra* note 40, at 17.
[313] *Id.*
[314] Helena Ursic ET AL., *supra* note 40, at 17; Peter Sayer, *LinkedIn blocked by Russian government*, PCWORLD (Nov. 17, 2016), https://www.pcworld.com/article/411055/isps-ordered-to-block-linkedin-in-russia.html.
[315] *LinkedIn blocked in Russia for violating provisions of "On the Procedure of Processing of Personal Data" Law of the Russian Federation*, SPECHT & PARTNER, https://www.specht-partner.com/linkedin/.

doi:10.6342/NTU202402499

access to LinkedIn.[316] This instance illustrates the trade barriers resulting from data localisation measures.

As previously discussed, local storage requirements are most likely to be inconsistent with GATS Articles XVI(a), (c), and Article XVII. Accordingly, this case study specifically discusses the following issue: Does the requirement for data controllers to store the data of Russian citizens within servers situated in Russia, as specified in Article 18.5 of the PDPL, affect the mode 1 supply of social network services and breach GATS Articles XVI(a), (c) and Article XVII?

A. Is Article 18.5 of the PDPL Covered by the GATS?

As previously introduced in Subsection A of this Chapter, GATS applies to measures affecting trade in services. Specifically, any measure taken by a Member state that affects the supply of a service, irrespective of whether the measure directly pertains to the supply of services or regulates other aspects, affects trade in services and shall be subject to the GATS.[317]

In this case, LinkedIn is banned by the Russian Federation because it failed to comply with the data storage requirement imposed by Article 18.5 of the PDPL (hereinafter "the measure at issue"). Therefore, the measure at issue does affect trade in services and thus is subject to the GATS.

B. The Measure at issue and GATS Article XVI:2 (a), (c)

As noted previously, market access is not a general discipline under the GATS. Members only need to abide by market access obligation when they make certain

[316] Lauren Mak & Chris Bluvshtein, *How to Unblock LinkedIn From Russia in 2024: A Full Guide*, VPNOVERVIEW (Mar. 18, 2024), https://vpnoverview.com/unblocking/censorship/access-linkedin-russia/#:~:text=Is%20LinkedIn%20allowed%20in%20Russia,Russia%20in%20a%20few%20steps.
[317] Panel Report, *EC — Bananas III*, ¶ 7.285.

doi:10.6342/NTU202402499

commitments in a particular mode of supply under specific service sectors in their GATS schedule. Therefore, it is critical to examine whether the service sectors and mode of supply affected by the measure at issue are subject to Members' commitment to market access.

a. How Should Social Networks Services Be Classified?

During the Uruguay Round negotiations, social networks on the internet did not exist, leading to their absence from classification regimes. Therefore, to classify social networks under the existing service classifications, one should evaluate the functions of individual social networks to find appropriate sub-categories.[318] To be sure, social networks indeed provide advertising services, which play a crucial role in meeting the financial needs of social networks and allow them to operate without charging users directly. However, advertising services are not the main interest of a social network user, who values the function of the social exchange of information more. Therefore, some scholars propose not to classify social network services as advertising services.[319]

Social network services could be qualified as "online storage and retrieval of data services" under the W/120 List. Particularly, database services under the "Computer and Related Services" sub-sector of business services (844) may be the most appropriate classification for social network services because (i) a social network's service is founded in a structured database and (ii) it is provided through communication networks, which are the two requirements of online storage and retrieval of data services.[320]

---

[318] ROLF H. WEBER & MIRA BURRI, CLASSIFICATION OF SERVICES IN THE DIGITAL ECONOMY 116 (2012).
[319] *Id.*
[320] *Id.* at 118 ("Database services under the "Computer and Related Services" sub-sector of business services (844): This sub-sector only knows one sub-class, namely all services provided from primarily structured databases through a communications network (8440), with the exclusion of data and message transmission services being classified in sub-class 7523. This definition shows that two requirements need to be fulfilled: (i) the service must be provided from primarily structured databases and, in addition (ii) it must be provided through a communication network.288 Looking at the services offered by a social

doi:10.6342/NTU202402499

b. Russia's Schedule of Commitment of CPC 84

According to Russia's Schedule of Specific Commitments[321] regarding Computer and Related Services, Russia commits to adhering to the market access obligation under Mode 1 supply without any limitations. Therefore, the measure at issue shall abide by GATS Article XVI(a) and (c).

c. Does the Measures at issue Limits Cross-border Social Networks Service Suppliers or Operations

The Appellate Body has clarified that any measure completely prohibiting service supply amounts to a market access limitation under Article XVI:2(a) and (c) because they reduce the number of service suppliers, operations, and output to zero.[322]

As discussed in Section I, Subsection B (a), some scholars argue that local storage requirements contradict the fundamental concept of cross-border service supply, leading to a zero quota for cross-border social network service suppliers operations because the necessity of storing data locally inherently requires service suppliers to operate data storage facilities within the territory.

Nonetheless, this thesis contends that the measure at issue does not necessarily restrict the number of cross-border social network service suppliers or their operations. This is because, besides LinkedIn, other cross-border social network service suppliers may already have data centers or storage facilities in Russia prior to the measure's

network it can be argued that the service is founded in a structured database and that it is provided through a communication network. Therefore, the sub-class 844 seems to be appropriate to classify the services of social networks as services covered by the "Computer and Related Services" sub-sector of the "Business Services" sector. In a given case, the specific Commitment Schedule of a country must be checked whether any commitments (without reservations and exclusions) have been assumed by the respective country.")

[321] Russian Federation Schedule of Specific Commitments, Trade in Services, GATS/SC/149, Nov. 5,2012.

[322] TOBIAS NAEF, *supra* note 72, 309.

doi:10.6342/NTU202402499

enforcement. Therefore, the measure may not necessarily constitute limitations under Article XVI:2(a) and (c).

Additionally, the use of local data centers or computing facilities does not inherently equate to a physical or commercial presence of service suppliers or service operations. Thus, the measure's consistency with GATS Article XVI:2(a) and (c) remains debatable.

C. The Measure at Issue and GATS Article XVII

As outlined in subsection B(c) of this chapter, GATS Article XVII:1 prohibits any Member from implementing measures that could give preferential treatment to domestic services and service suppliers over their foreign like counterparts. To ascertain whether the measure at issue provides a treatment less favorable to cross-border social network service and service suppliers compared to like domestic social network service and service suppliers, it is critical to address the following issues sequentially: (i) whether, and to what extent, there's a national treatment commitment for the specific services sector and mode of supply; (ii) whether the measure at issue imposed by a Member affects trade in services; (iii) whether the foreign and domestic services and service suppliers are 'like services and service suppliers'; (iv) and whether the foreign services and service suppliers are accorded "treatment no less favourable."

a. Russia's Schedule of Commitment

As noted above, social network services may be classified as "online storage and retrieval of data services" of "Computer and Related Services" (CPC844) under the W/120 List. According to Russia's Schedule of Specific Commitments,[323] regarding Computer and Related Services, Russia commits to adhering to the National Treatment

[323] Russian Federation Schedule of Specific Commitments, Trade in Services, WTO Doc GATS/SC/149, Nov. 5,2012.

doi:10.6342/NTU202402499

obligation under Mode 1 without any limitations. Hence, Russia commits to adhere to GATS Article XVII in its Schedule of commitments.

b. The Measure at Issue Affects Trade in Services

As previously discussed, the measure at issue does affect trade in services by imposing local data storage costs for foreign service suppliers such as LinkedIn, which do not store data in Russia prior to the measure's enforcement.

c. Likeness Criteria

In the *Argentina – Financial Services (2016)* case, the Appellate Body clarified that determining "likeness" under the GATS involves considering three factors: (1) characteristics of services and service suppliers, (2) consumers' preferences regarding services and service suppliers, and (3) tariff classification and description of services, such as those found in the UN Central Product Classification (CPC).

In this case, Russian domestic social network services such as *VKontakte*,[324] are like domestic services and service suppliers due to their similar characteristics with cross-border social network services and service providers. Moreover, consumer preferences for these domestic social network services mirror those for cross-border counterparts. Additionally, domestic social network services like *VKontakte* may also be categorized as "online storage and retrieval of data services" within the "Computer and Related Services" classification under the W/120 List.

d. Less Favourable Treatment Criteria

[324] *Russia's Leading Social Media Platform VK Has Been Expanding Fast, but at a Cost*, INTELLINEWS (Mar. 27, 2023), https://www.intellinews.com/russia-s-leading-social-media-platform-vk-has-been-expanding-fast-but-at-a-cost-274048// (last visited Apr. 10, 2024).

doi:10.6342/NTU202402499

Both *de jure* and *de facto* discriminatory measures are subject to the national treatment rule.[325] As previously introduced in this Chapter, Section II, Subsection C, the formally identical treatment accorded to both foreign like services and service suppliers and their domestic like counterparts can still be considered less favourable if it modifies the conditions of competition in favour of domestic services or service suppliers of the Member compared to like services or service suppliers of any other Member.

In this case, the measure at issue accords formal identical treatment to both cross-border social network service suppliers and their domestic like counterparts by requiring any data controllers who possess Russian citizens' personal data to store such data exclusively on servers situated within Russian territory.[326]

Accordingly, the measure at issue inevitably incurs compliance costs for social network service suppliers without data storage facilities in Russia. Therefore, the measure at issue modifies the competitive conditions to the advantage of like domestic suppliers of social network services only if they do not incur these compliance costs while their foreign counterparts do.

However, if this scenario does not occur, it is debatable whether the measure accords less favorable treatment to cross-border foreign social network services and suppliers. Therefore, the measure's consistency with GATS Article XVII relies on the market conditions related to data storage facilities used by both domestic and cross-border foreign social network services and suppliers in Russia.

---

[325] VAN DEN BOSSCHE & ZDOUC, *supra* note 16, at 401.

[326] *Russia's New Personal Data Localization Law Goes into Effect in September 2015*, DUANE MORRIS (June 15, 2015), https://www.duanemorris.com/alerts/russia_new_personal_data_localization_law_into_effect_september_2015_0615.html.

doi:10.6342/NTU202402499

D. The Measure at Issue and GATS Article XIV

If the measure is found inconsistent with the aforementioned obligations, as previously introduced in this Chapter, Section II, Subsection (C)(a), GATS Article XIV includes provisions for exceptions allowing Members to deviate from their obligations.

GATS Article XIV sets forth a two-tier test as follows: (i) whether the challenged measure falls within the scope of one of the paragraphs of Article XIV, and (ii) whether the challenged measure satisfies the requirements outlined in the chapeau of Article XIV.

a. GATS Article XIV(C)(ii) may be Invoked as Justification.

GATS Article XIV(c)(ii) justifies measures that are necessary to secure compliance with laws or regulations that are not inconsistent with the provisions of this Agreement including those relating to the protection of the privacy of individuals about the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts. In *Argentina — Financial Services (2016)*, the Appellate Body clarified the requirements of Article XIV of the GATS, focusing on two key elements: (i) the assessment of the measure's design to secure compliance and (ii) its necessity. [327]

In this case, the measure at issue, if found inconsistent with GATS Article XVI:2(a), (c), or Article XVII, may still be justified if (i) it is designed to secure compliance with laws or regulations that are not inconsistent with the provisions of this Agreement, including those relating to the protection of the privacy of individuals in relation to the processing and dissemination of personal data; and (ii) it meets the necessity requirement.

i. Designed to Secure the Compliance

[327] Appellate Body Report, *Argentina — Financial Services*, ¶ 6.202.

doi:10.6342/NTU202402499

In *Colombia — Textiles (2016)*, the Appellate Body asserted that the measure at issue is "designed" to secure compliance with laws or regulations that are not WTO-inconsistent when it is "not incapable of securing compliance therewith". Moreover, when the measure is "designed" to secure compliance, the panel should have proceeded to the "necessity" element of the analysis.[328]

In this case, Russia may contend that the measures at issue are designed to secure the compliance of the following data protection-related legislation that is not inconsistent with the GATS.

First of all, the Constitution of the Russian Federation stipulates the right to private life and personal data protection as fundamental rights of Russian citizens. Article 23:1 provides that "everyone shall have the right to the inviolability of his (her) private life, personal and family privacy, and protection of his (her) honour and good name.";[329] and Article 24:1 lays down that "Collecting, keeping, using and disseminating information about the private life of a person shall not be permitted without his (her) consent."[330] Secondly, Article 2 of the PDPL outlines that "the purpose of this Federal Law is to provide protection of human rights and liberties while processing personal data, including the right of integrity, personal and family secrecy."[331] The aforementioned laws are not inconsistent with GATS because they do not breach Russia's obligations thereunder.

Therefore, Russia may contend that the measure at issue is designed to secure compliance with Article 23:1, Article 24:1 of the Constitution of the Russian Federation, and Article 2 of the PDPL. Requiring data controllers to store the personal data of Russian citizens within Russia's borders aids Roskomnadzor in monitoring whether these data

[328] Appellate Body Report, *Colombia — Textiles (2016)*, ¶¶ 6.81–6.85 & 6.89.
[329] Constitution of the Russian Federation, Dec. 12, 1993, art. 23 ¶ 1.
[330] *Id.* art. 24 ¶ 1.
[331] Russian Federation Federal Law on Personal Data, 2014 (No. 242-FZ).

doi:10.6342/NTU202402499

controllers protect Russian citizens' privacy and private information properly, which can ensure the safety and confidentiality of Russian citizens' personal information. Therefore, the measure at issue is designed to secure compliance with Article 2, Article 5:1, and other provisions concerning data processing requirements outlined in the Personal Data Processing Law.

Nonetheless, some academics contend that the requirement to uphold an extra database within Russia exposes the personal data of Russian citizens to increased vulnerabilities, offering hackers an additional point of entry and raising various security concerns.[332] Given the measure at issue can be deemed "designed" to secure compliance with laws or regulations that are not WTO-inconsistent as long as it is "not incapable of securing compliance therewith," it is likely that the WTO panel will proceed to the "necessity" element of the analysis for addressing the said concern.

ii. The Necessity Requirement

As for the necessity test, the assessment begins with evaluating the relative importance of the interests or values promoted by the measure. Subsequently, the panel considers additional factors such as the measure's contribution to achieving its objectives and its impact on international commerce. A comparison between the challenged measure and possible alternatives is then conducted, with the results weighed against the significance of the interests at stake. Based on this comprehensive analysis, the panel determines whether the measure is necessary or if there exists another less trade-restrictive measure that is reasonably available.[333]

[332] Helena Ursic ET AL., *supra* note 40, at 11.
[333] VAN DEN BOSSCHE & ZDOUC, *supra* note 16, at 614.

doi:10.6342/NTU202402499

In determining whether an alternative measure that is less restrictive to trade is "reasonably available" to the Members, such measure shall reach the level of protection desired by the Member[334] and not impose an undue burden on that Member, such as prohibitive costs or substantial technical difficulties.[335]

The burden of proof lies with the responding party to demonstrate the measure's necessity, but they are not required to identify all theoretically possible reasonably available alternative measures.[336] Instead, only when the complaining party presents a less trade-restrictive alternative that is reasonably available would the burden shift to the responding party to justify the necessity of their measure compared to the proposed alternative.[337]

In this case, the acknowledgment of the significance of safeguarding personal data and privacy is widely accepted by WTO Members without dispute. However, the contentious issue is determining whether mandating local data storage is the least trade-restrictive measure to achieve this objective. Based on the established "necessity test" within WTO case law, Russia bears the burden of proving that the proposed less trade-restrictive alternative by the complainant is neither reasonably available nor could provide an equivalent level of personal data protection as the requirement for local data storage.

While less trade-restrictive alternatives may include requirements such as data encryption, securing databases with appropriate authentication measures, and

[334] Appellate Body Report, *EC — Asbestos (2001)*, ¶ 174.
[335] Appellate Body Report, *Brazil — Measures Affecting Imports of Retreaded Tyres*, WTO Doc WT/DS285/AB/R (adopted on Apr. 20, 2005), [hereinafter Appellate Body Report, *Brazil — Retreaded Tyres (2007)*], ¶ 156, citing Appellate Body Report, *US –Gambling (2005)*, ¶ 308.
[336] Appellate Body Report, *US — Gambling,* ¶ 309-11.
[337] *Id.*

doi:10.6342/NTU202402499

implementing adequate access control mechanisms, [338] Russia may contend that none of these alternatives can achieve the same level of protection, particularly when immediate access to data is required or necessary for achieving their national objectives.

Hence, GATS Article XIV(C)(ii) can still serve as a potential justification if the measure at issue is found to be inconsistent with Russia's obligations under GATS.

b. Whether the Measure at Issue is Consistent with the Chapeau of GATS Article XIV.

The chapeau of the GATS prohibits that a measure should not be "applied in a manner that constitutes arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on international trade".

In the *US — Shrimp*, the Appellate Body clarified that the measure in question must demonstrate the discriminatory application to establish "arbitrary or unjustifiable discrimination." [339] Concerning the element of "where the same conditions prevail between countries," arbitrary or unjustifiable discrimination can occur not only between exporting Members but also between exporting Members and the importing Member.[340]

Accordingly, the measure at issue is not inconsistent with the chapeau of GATS Article XIV when it is not applied in arbitrary or unjustifiable manner between Russia and other WTO members where like conditions prevail. Given the measure at issue aims to ensure the protection of Russian citizens' personal data by local storage requirements,

[338] *See generally* Habeeb Omotunde & Maryam Ahmed, *A comprehensive review of security measures in database systems: Assessing authentication, access control, and beyond*, 2023 MESOPOTAMIAN J. CYBERSECURITY 115 (2023), 115-133.
[339] Appellate Body Report, *United States — Import Prohibition of Certain Shrimp and Shrimp Products*, WT/DS58/AB/R (adopted on November 6, 1998), [hereinafter Appellate Body Report, *US — Shrimp (1998)*], ¶ 150.
[340] Appellate Body Report, *US — Shrimp (1998)*, ¶ 150.

doi:10.6342/NTU202402499

it shall apply to any data controllers possessing these personal data regardless of their nationality.

Hence, if Russia selectively enforces the measure at issue only on data controllers from specific nations, then the measure at issue is inconsistent with the chapeau of GATS Article XIV.

E. The Measure at issue and GATS Article XIV *bis*

GATS Article XIV *bis* is equivalent to Article XXI of the GATT, which has been commonly understood as "self-judging" due to the phrase "action which it considers necessary" in its wording.[341] Therefore, if the measure is found inconsistent with GATS obligations, Russia may contend that GATS Article XIV *bis* (1)(b)(iii) can justify such deviations.

Nonetheless, in the *Russia — Traffic in Transit* case, the Panel asserted that the subparagraphs of GATT Article XXI shall be subject to review by the WTO adjudicative body based on objective determinations.[342] In the recent *US — Origin Marking (Hong Kong, China)*, the Panel further claimed that GATT Article XXI(b)(iii) would only be invoked as a justification for measures inconsistent with GATT rules in situations of "utmost gravity" that could lead to a "breakdown or near-breakdown" in relations between the disputing parties.[343]

Similarly, when Russia aims to invoke GATS Article XIV *bis* (1)(b)(iii) as a justification, the measure at issue needs to be implemented during a "breakdown or near-

[341] *See* Roger P. Alford, *supra* note 418, at 702.
[342] Panel Report, *Russia — Traffic in Transit*, ¶ 7.101.
[343] Panel Report, *United States — Origin Marking Requirement,* WT/DS597/R, [hereinafter Panel Report, *United States — Origin Marking Requirement*], ¶ 7.289.

doi:10.6342/NTU202402499

breakdown" in relations between the disputing parties. Therefore, invoking GATS Article XIV *bis* (1)(b)(iii) is a challenging path when the measure at issue violates GATS obligations.

F. Insights from the Case Study

This case study highlights some inadequacy in GATS in regulating the negative trade impacts of local storage requirements.

First, local storage requirements might incur compliance costs for data controllers lacking local storage facilities. After all, mandating that data be stored locally necessitates the use of local data servers or facilities by affected service suppliers. While some scholars argue that these requirements effectively create zero quotas for cross-border service suppliers and operations under GATS Article XVI:2 (a) and (c), this assertion remains debatable since local storage facilities do not necessarily equate to the commercial or physical presence of service suppliers or operations.

Second, local storage requirements may impose additional compliance costs on both domestic and foreign services lacking local data servers for storage. However, even in such cases, local storage requirements are not necessarily inconsistent with GATS Article XVII:1 because they do not necessarily modify the competitive relationships between domestic and foreign like services and service suppliers, and thus, their negative impacts cannot be adequately addressed.

Third, GATS Articles XVI and XVII apply only to specific service sectors' modes of supply where members have undertaken commitments in their GATS Services Schedule. Therefore, GATS cannot mitigate the trade impact of these requirements on some services and service suppliers when such commitments are absent.

doi:10.6342/NTU202402499

In addition, even if local storage requirements are found inconsistent with members' obligations under the GATS, GATS Article XIV(c)(ii) is likely to serve as a justification for them. It is also worth noting that while national security is a common rationale for governments to impose local storage requirements, it is less likely to justify deviations from GATS under Article XIV *bis*. This is because the Panel no longer considers the national security exception as entirely self-judging, and the threshold for meeting the subparagraphs of GATS Article XIV bis is quite high.

To sum up, GATS may not be sufficient to address the trade impact resulting from local storage requirements. Hence, this thesis aims to further explore the possibility of explicitly restraining or even prohibiting local storage requirements within the future WTO legal framework. This exploration involves examining such discussions raised in the negotiation progress of the WTO e-commerce work programme in the subsequent Section.

III. The Negotiation Progress under the WTO Legal Forum in Terms of E-Commerce.

A. Introduction to the WTO work program on E-commerce.

The GATS was established before the electronic commerce emerged as a prominent global economic issue.[344] Recognizing the growth and potential of global electronic commerce, the WTO incorporated "e-commerce" into its agenda with the adoption of the Declaration on Global Electronic Commerce in 1998.[345] Electronic commerce, or e-

[344] *See* Xiaolian Quan, *The Governance of Cross-Border Data Flows in Trade Agreements: Is the CPTPP Framework an Ideal Way out*, 15 FRONTIERS L. CHINA 253 (2020), at 257.
[345] World Trade Organization, Ministerial Declaration of 20 May 1998 on Global Electronic Commerce, WTO Doc. WT/MIN (98) /DEC/2, [hereinafter Ministerial Declaration on E-Commerce], https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?CatalogueIdList=4814,34856,20308&CurrentCatalogueIdIndex=1.

doi:10.6342/NTU202402499

commerce, is defined as the "production, distribution, marketing, sale or delivery of goods and services by electronic means" in this context.[346]

Data-related issues have been a component of electronic commerce negotiations within the WTO since 1998.[347] These negotiations have evolved through four distinct phases: the preparatory phase until 2015, the departure from the Doha framework from 2015 to 2017, the Joint Statement Initiative from 2017 to 2019, and the ongoing negotiations that began in 2019.[348]

a. Preparatory Work

The WTO's 1998 Work Programme was initiated with an exploratory and informative purpose.[349] It assigned four WTO bodies the task of examining how existing WTO agreements relate to e-commerce, including the Council for Trade in Services.[350] Discussions on e-commerce were initially scattered across the Council for Trade in Services, the Council for Trade in Goods, the Council for Trade-Related Aspects of Intellectual Property Rights (hereinafter "TRIPs"), and the Committee on Trade and Development.[351]

---

[346] *Electronic commerce*, WORLD TRADE ORGANIZATION, https://www.wto.org/english/thewto_e/minist_e/mc11_e/briefing_notes_e/bfecom_e.htm(last visited Mar. 19, 2024).
[347] TOBIAS NAEF, *supra* note 72, at 284.
[348] *Id.*
[349] YASMIN ISMAIL, E-COMMERCE IN THE WORLD TRADE ORGANIZATION: HISTORY AND LATEST DEVELOPMENTS IN THE NEGOTIATIONS UNDER THE JOINT STATEMENT 9 (2020), https://www.iisd.org/system/files/publications/e-commerce-world-trade-organization-.pdf.
[350] Ministerial Declaration on E-Commerce.
[351] Council for Trade in Services, *Work Programme on Electronic Commerce - interim report to the General Council*, WTO Doc. S/C/8 (Mar. 31, 1999); TRIPS Council, *Interim review of progress in the implementation of the Work Programme on Electronic Commerce – Communication from the Chairman of the Council for TRIPS,* WTO Doc. WT/GC/21 (Mar. 23, 1999); Committee on Trade and Development, *Interim review of progress in the implementation of the Work Programme on Electronic Commerce - Communication from the Chairman of the Committee on Trade and Development,* WTO Doc. WT/GC/23 (Apr. 7, 1999); Council for Trade in Goods, *Interim review of progress in the implementation of the Work Programme on Electronic Commerce - Communication from the Chairman of the Council for Trade in Goods,* WTO Doc. WT/GC/24 (Apr. 9, 1999).

doi:10.6342/NTU202402499

The issue concerning the relationship between trade and data localisation first emerged within the e-commerce work programme for Council for Trade in Services in May 2014.[352] This initiative was introduced by representatives from the US, along with the discussions on data flows.[353] On December 17, 2014, the US submitted a communication paper to the Council for Trade in Services.[354] In this submission, the US highlighted that localization requirements can hinder cross-border data flows by mandating data be processed within specific national borders.[355] The paper also advocated for enhanced information sharing regarding policies that enforce localization.[356]

Although Members continued discussing data localization concerns in March 2015, several delegations emphasized that no new commitments or regulations could be negotiated as part of the e-commerce Work Programme.[357]

In summary, progress in implementing the Work Programme was limited before 2015 due to its preparatory phase and the deadlock of the Doha Round negotiations.[358] Nonetheless, towards the end of this preparatory period, concerns among Members regarding data localization began to emerge.

b. Departure From the Doha Structure

In December 2015 at Nairobi, the Tenth Ministerial Conference acknowledged the interest of certain Members in exploring alternative approaches to negotiations instead of

[352] Council for Trade in Services, *Work Programme on Electronic Commerce - Report by the Chairman of the Council for Trade in Services to the General Council,* WTO Doc S/C/43 (June 30, 2014).
[353] *Id.*
[354] Council for Trade in Services, *Work Programme on Electronic Commerce – Communication by the United States,* WTO Doc S/C/W/359 (Dec. 17, 2014).
[355] *Id.* ¶ 4.4.
[356] *Id.* ¶ 4.6.
[357] Council for Trade in Services, *Work Programme on Electronic Commerce – Report by the Chairman of the Council for Trade in Services to the General Council,* WTO Doc S/C/47 (July 17, 2015).
[358] Ismail, *supra* note 343, at 9.

doi:10.6342/NTU202402499

adhering to the existing Doha negotiation structure.[359] However, the Nairobi Declaration emphasized that any decision to initiate multilateral negotiations on new issues to be discussed, would require unanimous agreement from all Members.[360]

In 2016 and 2017, significant discussions and initiatives regarding e-commerce unfolded within the framework of the WTO.[361] Mexico, Indonesia, South Korea, Turkey, and Australia became the MIKTA Group, which convened a workshop on July 5, 2016, at the WTO, emphasizing the necessity for the organization to dedicate more attention to its digital trade agenda.[362] Data localisation had been identified as a new relevant issue to trade policies.[363]

Leading up to the Eleventh Ministerial Conference in Buenos Aires, discussions within the WTO's Work Programme intensified. The US had advocated for a prohibition on data localization to prevent companies and digital entrepreneurs who rely on cloud computing from having to build physical infrastructure and expensive data centers in every market.[364] Canada, Chile, Colombia, Côte d'Ivoire, the EU, the Republic of Korea, Mexico, Montenegro, Paraguay, Singapore, and Turkey proposed a joint communication which requests to ensure cross-border data flows and data localisation disciplines building on existing WTO commitments and subject to appropriate public policy exceptions.[365]

---

[359] Ministerial Conference, *Nairobi Ministerial Decision*, WTO Doc. WT/MIN(15)/DEC (Dec. 21, 2015), ¶ 30.
[360] *Id.* ¶ 34.
[361] Ismail, *supra* note 343, at 12.
[362] MIKTA, *MIKTA e-commerce workshop reflections* (Aug. 8, 2016), http://mikta.org/document/mikta-e-commerce-workshop-reflections/ (last visited at July 8, 2024).
[363] *Id.* ("There are also newer E-Commerce issues that have only come onto the trade policy radar in recent years, such as data flows and data localization technical work is needed to increase understanding about various trade policy approaches and their implications for developed and developing countries; to build comfort around the types of trade disciplines that could be negotiated;")
[364] General Council, Work Programme on Electronic Commerce, *Non-paper from the United States*, WTO Doc JOB/GC/94 (July 4, 2016), ¶ 2.5.
[365] General Council, Council for Trade in Goods, Council for Trade in Services, Council for Trade-Related Aspects of Intellectual Property Rights, Committee on Trade and Development, *Work Programme on Electronic Commerce, Trade Policy, the WTO, and the Digital Economy, Communication from*

doi:10.6342/NTU202402499

However, some developing countries, especially African nations, were against the idea of negotiating new rules.[366] Following the Nairobi Declaration, discussions surrounding e-commerce gained momentum leading to the launch of exploratory talks on potential trade rules for electronic commerce by 71 Members during the WTO's 2017 Buenos Aires Ministerial Conference.[367] Subsequently, an enlarged version of this group endorsed a second Joint Statement in Davos in January 2019, signaling the signatories' intention to commence negotiations.[368]

c. The First Joint Statement Initiative

This phase of negotiation following the signing of the first Joint Statement Initiative (hereinafter "JSI") in December 2017 at the MC11 of Buenos Aires marked a series of meetings and changes in participation.[369] Initially, on 13 December 2017, a group of 71 WTO Members led by the US, EU, and Japan consented to begin exploratory work aimed at future WTO negotiations concerning trade-related aspects of e-commerce.[370] Co-sponsorship of JSI shifted over time, with several countries leaving or joining the initiative.[371] Notably, all developed countries are part of the JSI, while only three LDCs joined and five African WTO Members co-sponsored it.[372]

Canada, Chile, Colombia, Côte d'Ivoire, the EU, the Republic of Korea, Mexico, Montenegro, Paraguay, Singapore and Turkey, WTO Doc JOB/GC/116, JOB/CTG/4 JOB/SERV/248, JOB/IP/21 JOB/DEV/42 (Jan. 13, 2017), ¶ 20.

[366] General Council, *Work Programme on Electronic Commerce - Report of panel discussion on "digital industrial policy and development" - Communication from the African Group,* WTO Doc JOB/GC/133 (July 21, 2017).

[367] Ministerial Conference, *Joint Statement on Electronic Commerce*, WTO Doc WT/MIN(17)/60 (Dec. 13, 2017), [hereinafter first JSI].

[368] Joint Statement on Electronic Commerce, WTO Doc. WT/L/1056 (Jan. 25, 2019), [hereinafter second JSI].

[369] WTO, *New initiatives on electronic commerce, investment facilitation and MSME* (Dec. 13, 2017), https://www.wto.org/english/news_e/news17_e/minis_13dec17_e.htm (last visited Apr. 11, 2024).

[370] First JSI.

[371] Ismail, *supra* note 343, at 14

[372] Ismail, *supra* note 343, at 14.

doi:10.6342/NTU202402499

Data localisation also stands out as a proposed issue for inclusion in the forthcoming e-commerce agreement. For instance, Japan proposed adopting a two-pronged approach to regulate mandatory requirements on the location of servers.[373] This approach involves a general prohibition on such requirements, coupled with exceptions permitting Members to achieve legitimate public policy objectives.[374] Japan specifically highlights the barriers to market access for foreign businesses posed by these requirements as a rationale for prohibiting such requirements.

d. The Second Joint Statement Initiative

As of February 2020, seven negotiation rounds had concluded, engaging over 80 WTO Members.[375] Significant disparities have emerged among three key WTO influencers, the US, China, and the EU, particularly concerning topics such as data protection and data flow issues.[376]

i. The US Position

The US has been at the forefront of advocating for digital trade standards within WTO e-commerce discussions. The US proposal outlining trade provisions aimed at safeguarding and promoting digital trade[377] and is also designed to foster an open, fair, and competitive digital economy environment that benefits both developed and

[373] Japan JSI Proposal, ¶ 3.8 ("As cross-border data transfer becomes an essential part of business practices. Companies take strategic decisions on the locations of computing facilities, taking into account the cost and efficiency of operations, while at the same time hedging various risks. In such contexts, mandatory requirements by a government to locate servers within its territory would discourage companies from entering into its market due to the increased cost and risk associated with such requirements. Therefore, it would be worth considering reaching an agreement among Members in the WTO in which, with the exception of cases to achieve a legitimate public policy objective, governments should not impose mandatory requirements on the location of servers, as such requirements pose critical barriers to entry into the market by foreign businesses.").
[374] *Id.*
[375] Rachel F. Fefer, *Internet Regimes and WTO E Commerce Negotiations*, EVERYCRSREPORT (Jan. 28, 2020), at 19-22, https://crsreports.congress.gov/product/pdf/R/R46198/1.
[376] *Id.*
[377] US JSI Proposal, ¶ 1.2.

doi:10.6342/NTU202402499

developing countries.[378] The US highlights the pivotal role of cross-border data flows in global trade, citing McKinsey Global Institute's assessment that these flows generated $2.8 trillion in economic value in 2014, surpassing the impact of global trade in goods on world GDP.[379] To bolster economic growth, the US advocates for trade rules that uphold the unrestricted data flow while implementing reasonable safeguards, such as consumer data protection.[380]

The proposed rules concerning data flow consist of three main components, namely: (i) Cross-Border Transfer of Data: The US proposes trade regulations that ensure both consumers and companies have the freedom to transfer data across borders without facing arbitrary or discriminatory restrictions; (ii) Preventing Data Localisation: the US suggests regulations that prohibit the imposition of requirements on companies to construct digital infrastructure in every jurisdiction they operate in, thereby enabling more efficient customer service; and (iii) Prohibiting Web Blocking.[381]

In sum, the US proposal concerning data localisation issues reflects its regulatory models that advocate for business-led development. It advocates for trade rules that prohibit data localisation to enable Internet-enabled services to lower costs and enhance customer services.

ii. The Chinese Position

China's proposal for e-commerce within the WTO emphasizes facilitating digital trade and global value chains, particularly to benefit developing nations, which aligns

[378] *Id.*
[379] *Id*. ¶ 2.
[380] *Id.*
[381] *Id (*"Preventing Data Localization: The economies of scale afforded by Internet-enabled services reduce costs, improve quality of service, and strengthen cybersecurity for firms. Trade rules can ensure that companies are not required to build or employ unique, capital-intensive digital infrastructure in every jurisdiction they serve, allowing them to better serve their customers.").

doi:10.6342/NTU202402499

with its state-driven approach.[382] Unlike the U.S., which seeks firm commitments on data flows, China advocates for respecting each other's design of the electronic commerce development paths and considering varying levels of industrial development and cultural traditions among Members.[383]

Specifically, China prioritizes respect for internet sovereignty, data security, and privacy policies and advocates for flexibility in regulatory measures to achieve reasonable public policy objectives.[384] It suggests exploratory discussions rather than firm commitments on data flows and digital product treatment.[385] Overall, the Chinese proposal highlights the state-centric regulatory models in terms of data flows and does not include the proposal prohibiting data localisation measures.

iii. The EU Position

[382] Joint Statement on Electronic Commerce Initiative: Communication from China, WTO Doc. INF/ECOM/19 (Apr. 23, 2019) [hereinafter China JSI Proposal], ¶ 2.2 ("WTO negotiation on electronic commerce should be committed to tapping into the great potential of electronic commerce, helping Members, particularly developing Members and LDCs, to integrate into global value chains, bridge the digital divide, seize development opportunities and benefit from inclusive trade, and hence better participating in the economic globalization."), ¶ 4.3 ("It's undeniable that trade-related aspects of data flow are of great importance to trade development. However, more importantly, the data flow should be subject to the precondition of security, which concerns each and every Member's core interests. To this end, it is necessary that the data flow orderly in compliance with Members' respective laws and regulations.").

[383] *Id.* ¶ 4.1 ("Along with the new opportunities provided by electronic commerce, issues such as cyber security, data safety and privacy are increasingly highlighted, bringing unprecedented security risks and regulatory challenges to Members. Members sponsoring the Davos Joint Statement include not only developed Members, but also developing Members and LDCs. They differ in national conditions and development stages, have different challenges and concerns on electronic commerce-related issues. When it comes to the entire WTO membership, the interests are even more diversified. Therefore, to advance the negotiation, differences in Members' respective industry development conditions, historical and cultural traditions as well as legal systems need to be fully understood. Bearing in mind the aforementioned differences, Members should respect each other's design of the electronic commerce development paths, and the legitimate right to adopt regulatory measures in order to achieve reasonable public policy objectives.")

[384] China JSI Proposal, ¶4.1

[385] *Id.* ¶ 4.2 ("In the exploratory discussions, some Members mentioned digital trade rules, covering issues such as data flow, data storage, treatment of digital products, etc. In light of their complexity and sensitivity, as well as the vastly divergent views among the Members, more exploratory discussions are needed before bringing such issues to the WTO negotiation, so as to allow Members to fully understand their implications and impacts, as well as related challenges and opportunities.")

doi:10.6342/NTU202402499

The EU's proposal for digital trade regulations positions itself between the approaches of the US and China. On the one hand, it advocates for a "comprehensive and ambitious set of WTO disciplines and commitments" covering e-commerce, consumer protection, personal data protection, and cross-border data flows.[386] On the other hand, aligned with its domestic policy priorities, the EU emphasizes the protection of personal privacy.[387] In terms of data flow issues, the EU opposes any restrictions on cross-border data flows that impede trade in the digital economy.[388] Specifically, it prohibits requirements such as mandating the use of local computing facilities or network elements for data processing, compelling data localisation within the EU's territory, prohibiting storage or processing in other countries' territories, or conditioning cross-border data transfers on the use of specific computing facilities or network elements.[389]

Nonetheless, the EU also allows Members to adopt and maintain safeguards for personal data protection.[390] The EU acknowledges that safeguarding personal data is a fundamental right essential for fostering trust in the digital economy and promoting trade development.[391] Accordingly, Members should have the discretion to establish and uphold measures they deem appropriate to protect personal data and privacy, including

[386] Joint Statement on Electronic Commerce Initiative: Communication from European Union, WTO Doc INF/ECOM/22 (Apr. 26, 2019) [hereinafter EU JSI Proposal], ¶ 1.1 ("The EU is fully committed to ongoing WTO negotiations on e-commerce. In this context, it will seek to negotiate a comprehensive and ambitious set of WTO disciplines and commitments, to be endorsed by as many WTO Members as possible. The EU supports the open, transparent and inclusive character of these negotiations.")
[387] *Id.* ¶ 2.8.
[388] *Id.* ¶ 2.7("Members are committed to ensuring cross-border data flows to facilitate trade in the digital economy. To that end, cross-border data flows shall not be restricted by:(a) requiring the use of computing facilities or network elements in the Member's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of the Member;(b) requiring the localization of data in the Member's territory for storage or processing; (c) prohibiting storage or processing in the territory of other Members; (d) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Member's territory or upon localization requirements in the Member's territory.").
[389] EU JSI Proposal, ¶ 2.7.
[390] *Id.* ¶ 2.8.
[391] *Id.* ¶ 2.8.1.

doi:10.6342/NTU202402499

rules governing the cross-border transfer of such data.[392] The EU emphasizes that no agreed disciplines should undermine the protections already in place for personal data within each Member's jurisdiction.[393]

In other words, the EU proposal supports Members in restricting or prohibiting cross-border data flows when deemed necessary for personal data protection. Critics argue that this could undermine the commitment to cross-border data flows because it potentially permits Members to impose restrictions in the name of privacy protection.[394]

In sum, the EU's proposal underscores its mixed economy model which seeks an equilibrium between safeguarding personal privacy and facilitating unrestricted data movement. Regarding local storage requirements, the EU only proposes banning such requirements if they become constraints on cross-border data transfers, which highlights their primary concerns over data localization policies centered around issues of data mobility.

B. Current Negotiation Progress.

Currently, 90 WTO Members, representing over 90% of global trade, are engaged in formal negotiations under the JSI.[395] While comprising only 55% of total WTO Membership, this group encompasses numerous major trading Members, with their trade constituting over 90% of global trade.[396] However, participation from developing

[392] *Id.* ¶ 2.8.2.
[393] *Id.*
[394] Fefer RF (2020), at 20.
[395] Yasmin Ismail & Rashmi Jose, *E-Commerce Takes Centre Stage at World Trade Organization in Run-up to MC13*, INT'L INST. FOR SUSTAINABLE DEV. (Jan. 11, 2024), https://www.iisd.org/Art.s/policy-analysis/e-commerce-developments-wto-mc13(last visited Apr. 10, 2024).
[396] *Id.*

doi:10.6342/NTU202402499

economies and LDCs is limited, with only eight African and five LDC Members involved.[397]

The negotiations have encountered challenges in reconciling different Member positions on various issues, such as data flow, data localisation, or location of computing facilities.[398] Notably, the US was the main advocate of the free flow of data and the prohibition of data localisation within the JSI negotiation. However, the US withdrew support for proposals on these issues in October 2023, leading to the pending discussion on the draft article on data localisation.[399]

Regarding the EU's stance, they propose preventing data localization measures that restrict cross-border data flows. However, the EU's concern does not extend to local storage requirements that allow cross-border data flows. Additionally, the EU advocates for exceptions that permit Members to restrict or prohibit cross-border data flows when they deem appropriate to protect personal data.

The EU's choice of wording, "deem appropriate," in its JSI proposal mirrors the language "consider necessary" found in GATS Article XIV *bis* (1)(b). This suggests that the EU intends to propose personal data protection as a "self-judging" exception for Members to restrict cross-border data flows. Importantly, the criteria for this exception appear more flexible than those of GATS Article XIV *bis* (b), as Members only need to deem the measure "appropriate" rather than "necessary" to invoke the exception.

[397] *Id.*
[398] *Id.*
[399] Ismail & Jose, *supra* note 509.

doi:10.6342/NTU202402499

In contrast, the Chinese JSI proposal does not advocate for the prohibition of data localization measures and underscores a regulatory model centered around state control over data flows.

On November 15, 2023, an updated consolidated negotiating text has been issued to capture the progress in the JSI discussion.[400] Concerning the prohibition on data localisation measures, the most common proposed text is as follows:[401]

> 4. [Parties\Members] recognise that each [Party\Member] may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications.
>
> 5. [Unless otherwise provided for under its laws or regulations], [no\No] [Party/Member] shall require a covered person to use or locate computing facilities in that [Party's/Member's] territory as a condition for conducting business in that territory.
>
> 6. Nothing in this Article shall prevent a [Party/Member] from adopting or maintaining measures inconsistent with paragraph 5 to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on the use or location of computing facilities greater than are [necessary/required] to achieve the objective.

[400] WTO Electronoic Commerce Negotiations, Updated Consolidated Negotiation Text-November 2023, WTO Doc INF/ECOM/62/Rev.5 (Nov. 15, 2023).
[401] *Id.* at 32.

doi:10.6342/NTU202402499

In conclusion, amidst the negotiations involving these influential trade players, there remains no clear consensus on how to regulate local storage requirements within the JSI framework. The JSI discussions reflect the importance of grappling with balancing the imperatives of data protection, economic liberalization, and national regulatory interests. Nonetheless, after the US withdrew its proposal concerning prohibiting data localization, the proposed text did not appear in the draft chair's text issued on June 28, 2024.[402]

IV. Summary

Data controllers are obligated to store data within specific geographical regions under local storage requirements. Accordingly, local storage requirements invariably limit data controllers' strategic decisions on the locations of computing facilities,[403] incurring compliance costs for establishing or leasing local data centres or servers.

The said impact directly affects cross-border service suppliers lacking local storage facilities. Cross-border service supply, as defined in GATS Art. I:2(a), refers to services delivered by any service supplier located within its own country of one WTO Member to any customer residing in different jurisdictions governed by any other WTO Members.

Some scholars thus assert that local storage requirements are inconsistent with GATS Article XVI:2(a) and (c) because cross-border services do not require any physical presence of service suppliers or service operations within the territory where the services are delivered. However, it is debatable whether the requirement for local data servers or

[402] WTO Electronoic Commerce Negotiations, Draft Chair's Text, WTO Doc INF/ECOM/86 (June 28, 2024).
[403] *See* Japan JSI Proposal, ¶ 3.8.

doi:10.6342/NTU202402499

computing facilities constitutes a physical or commercial presence for service suppliers or operations.

In addition, local storage requirements do not necessarily favour domestic like services and service suppliers over their foreign competitors, and thus whether they constitute a violation of GATS Article XVII:1 depends on a case-by-case analysis.

Notably, both GATS Article XVI and XVII are only binding when Members commit to specific sectors' modes of service supply. Consequently, GATS may not sufficiently resolve the negative trade impact resulting from local storage requirements in any service sector.

GATS was formed before the rise of electronic commerce as a prominent global economic prosperity. Accordingly, the WTO incorporated e-commerce into its agenda with the adoption of the Declaration on Global Electronic Commerce in 1998, eventually leading to the formation of the plurilateral platform JSI.

In JSI's discussions, some Members have proposed prohibiting data localization, suggesting that the existing legal framework of the WTO may not fully address the trade implications of data localisation measures. Observations of communications submitted by WTO Members within the E-commerce work programme and the JSI indicate that those advocating for the prohibition of data localization primarily aim to reduce the costs businesses incur when investing in local data centers or computing facilities and to facilitate cross-border data flows.

However, achieving consensus has been challenging due to the differing positions held by influential parties such as the US, China, and the EU. Their divergent stances mainly result from the balance between business openness, data sovereignty, and data

doi:10.6342/NTU202402499

protection. Moreover, the withdrawal of the US proposal has left data localisation issues unresolved within the current negotiation progress of the JSI.

Overall, the JSI discussions indicate that some WTO members deem the current legal framework of the WTO is insufficient to mitigate the trade impact resulting from data localisation measures and propose trade rules restricting these measures. Nonetheless, how to balance national interests and trade liberalization is not thoroughly addressed in Members' proposal.

Consequently, in the subsequent Chapter, this thesis aims to draw regulatory insights from different regulatory models found in provisions prohibiting or restricting local storage requirements within various RTAs and DEAs.

doi:10.6342/NTU202402499

CHAPTER FOUR

RTAS AND DEAS AND LOCAL STORAGE REQUIREMENTS?

Current RTAs encompass provisions on the data localisation measures.[404] As of November 2023, there were 30 RTAs that included mandatory provisions prohibiting data localisation measures as a condition for conducting businesses.[405] Singapore, Australia, Chile, and Japan stand out among the countries with the highest number of such provisions.[406] These provisions, often categorized under headings such as "location of computing facilities," either prohibit or restrict data localisation practices, albeit with varying exceptions.[407] The first agreement including the prohibition clause on data

[404] *TAPED A Dataset on Digital Trade Provisions*, UNIV. LUCERNE, https://www.unilu.ch/en/faculties/faculty-of-law/professorships/burri-mira/research/taped/ (last visited Apr. 10, 2024); *TAPED Dataset (2023/11/02)*, UNIV. LUCERNE, https://www.unilu.ch/en/faculties/faculty-of-law/professorships/burri-mira/research/taped/ (last visited Apr. 10, 2024) [hereinaftere TAPED Dataset].

[405] *See* TAPED Dataset; *See* also TAPED Codebook (2023/11/02), UNIV. LUCERNE, at 28, https://www.unilu.ch/en/faculties/faculty-of-law/professorships/burri-mira/research/taped/(last visited Apr. 10, 2024) ("2.2.3 …This provision can be aimed at limiting or prohibiting the use of data localization requirements. The provision should be specific (i.e., for all types of data flows) and not a commitment that could cover such a barrier only in the case of trade in services or investment… 2: yes (hard)") (Select bottom number two from the first row of the colume "DL", entitled "data_flow_proh_loc_2_2_3" in the TAPED Dataset. The resulting Excel list shows 30 RTAs encompassing mandatory provisions that limit or prohibit the use of data localization requirements).

[406] CHIARA DEL GIOVANE ET AL., *supra* note 14, at 16.

[407] Agreement Between Japan and Mongolia for an Economic Partnership, Japan-Mongolia, Feb. 10, 2015, https://rtais.wto.org/UI/PublicShowMemberRTAIDCard.aspx?rtaid=835 (last visited Apr. 10, 2024) [hereinafter Japan–Mongolia FTA], art. 9.10; Transpacific Partnership Agreement, Feb. 4, 2016, https://ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-full-text (last visited Apr. 10, 2024) [hereinafter TPP], art. 14.13; Singapore Australia Free Trade Agreement, Singapore-Australia, Sep. 5, 2003, https://www.dfat.gov.au/trade/agreements/in-force/safta/official-documents (last visited Apr. 10, 2024) [hereinafter SAFTA], art. 24; Free Trade Agreement Between the Democratic Socialist Republic of Sri Lanka and the Republic of Singapore, Singapore-Sri Lanka, Jan. 23, 2018, https://edit.wti.org/document/show/290ae462-2914-4e19-b516-678bbcd4f8e1 (last visited Apr. 10, 2024) [hereinafter Singapore–Sri Lanka FTA], art.9.10; Peru Australia Free Trade Agreement, Peru-Australia, June 24, 2020, https://www.dfat.gov.au/trade/agreements/in-force/pafta/full-text/Pages/fta-text-and-associated-documents (last visited Apr. 10, 2024) [hereinafter Australia–Peru FTA], art. 13.12; Comprehensive and Progressive Agreement for Trans-Pacific Partnership, Mar. 8, 2018, https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/cptpp/comprehensive-and-progressive-agreement-for-trans-pacific-partnership-text-and-resources/ (last visited Apr. 10, 2024) [hereinafter CPTPP], art. 14.13; Agreement between the United States of America, the United Mexican States, and Canada, US-Mexico-Canada, Nov. 30, 2018, https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between (last visited Apr. 10, 2024) [hereinafter USMCA], art. 19.12; Free Trade Agreement between the Republic of Chile and the Federative Republic of Brazil, Brazil-Chile, Nov. 21, 2018, https://edit.wti.org/document/show/e62cfb4c-abbf-43d9-ae34-a15c7d057ab4 (last visited Apr. 10, 2024) [hereinafter Brazil–Chile FTA], art. 10.13; ASEAN Agreement on Electronic Commerce, Jan. 22, 2019, https://agreement.asean.org/media/download/20190306035048.pdf (last visited Apr. 10, 2024)

doi:10.6342/NTU202402499

localisation measures is the 2015 Agreement Between Japan and Mongolia for an Economic Partnership (hereinafter "Japan–Mongolia FTA"), according to which neither Party "shall require a service supplier of the other party, an investor of the other party, or an investment of an investor of the other party in the area of the former party, to use or locate computing facilities in that area as a condition for conducting its business."[408]

This chapter explores clauses that address data localisation measures in several prominent mega RTAs in section I. It then proceeds to present distinct legal strategies employed by the US, the European Union, and China in the clauses concerning local storage requirements in their respective RTAs in section II. In section III, this thesis aims

[hereinafter ASEAN E-commerce Agreement], art. 7; Indonesia Australia Comprehensive Economic Partnership Agreement, Indonesia–Australia, Mar. 4, 2019, https://www.dfat.gov.au/trade/agreements/in-force/iacepa/indonesia-australia-comprehensive-economic-partnership-agreement (last visited Apr. 10, 2024) [hereinafter Indonesia–Australia CEPA], art. 13.12; Australia Hong Kong Free Trade Agreement and Associated Investment Agreement, Hong kong-Australia, Mar. 26, 2019, https://www.dfat.gov.au/trade/agreements/in-force/a-hkfta/a-hkfta-text/Pages/default (last visited Apr. 10, 2024) [hereinafter Australia–Hong Kong FTA], art. 11.8; Agreement Between the United States of America and Japan Concerning Digital Trade, Japan-US, Oct. 7, 2019, https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf (last visited Apr. 10, 2024) [hereinafter Japan–US DTA], art. 12; Australia-Singapore Digital Economy Agreement, Australia-Singapore, Aug. 6, 2020, https://www.dfat.gov.au/trade/services-and-digital-trade/australia-and-singapore-digital-economy-agreement (last visited Apr. 10, 2024) [hereinafter ASDEA], art. 24; Regional Comprehensive Economic Partnership Agreement, Dec. 15, 2020, https://www.dfat.gov.au/trade/agreements/in-force/rcep/rcep-text (last visited Apr. 10, 2024) [hereinafter RCEP], art. 12.14; Digital Economy Partnership Agreement, Chile-New Zealand-Singapore, June 12, 2020, https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement-depa/depa-text-and-resources/ (last visited Apr. 10, 2024) [hereinafter DEPA], art. 4.4; Australia-United Kingdom Free Trade Agreement, Australia-United Kingdom, Dec. 17, 2021, https://www.dfat.gov.au/trade/agreements/in-force/aukfta/official-text (last visited Apr. 10, 2024) [hereinafter Australia–UK FTA], art. 14.11; Digital Economy Agreement between the United Kingdom of Great Britain and Northern Ireland and the Republic of Singapore, Singapore-UK, Feb. 25, 2022, https://www.gov.uk/government/collections/uk-singapore-digital-economy-agreement (last visited Apr. 10, 2024) [hereinafter Singapore–UK DEA], art. 8.61-G; Free Trade Agreement between the United Kingdom of Great Britain and Northern Ireland and New Zealand, New Zealand–UK, Feb. 28, 2022, https://www.gov.uk/government/collections/free-trade-agreement-between-the-united-kingdom-of-great-britain-and-northern-ireland-and-new-zealand (last visited Apr. 10, 2024) [hereinafter New Zealand–UK FTA], art. 15.15; Digital Partnership Agreement between the Government of the Republic of Korea and the Government of the Republic of Singapore, Korea-Singapore, Nov. 21, 2022, https://www.fta.go.kr/webmodule/_PSD_FTA/ksdpa/1/DPA_eng.pdf (last visited Apr. 10, 2024) [hereinafter Korea–Singapore DEA], art. 14.15; Digital Trade Agreement between the United Kingdom of Great Britain and Northern Ireland and Ukraine, UK–Ukraine, Mar. 20, 2023, https://www.gov.uk/government/publications/ukukraine-digital-trade-agreement-cs-ukraine-no22023 (last visited Apr. 12, 2024) [hereinafter UK–Ukraine Digital Trade Agreement].

[408] Japan–Mongolia FTA, art. 9.10.

doi:10.6342/NTU202402499

to uncover areas of regulatory convergence and divergence among the "location of computing facilities" provisions, which represent the predominant regulatory models governing the clauses prohibiting data localisation requirements in various RTAs.[409] Lastly, conclusions are drawn in section IV.

I. Mega RTAs or DEAs that prohibit local storage requirements.

This section will review and compare the general principles and exceptions governing local storage requirements in the Trans-Pacific Partnership, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership, the United States-Mexico-Canada Agreement, the Digital Economy Partnership Agreement between New Zealand, Singapore, and Chile, and the Regional Comprehensive Economic Partnership.

A. Trans-Pacific Partnership Agreement

The Trans-Pacific Partnership (hereinafter "TPP"), initially signed in 2005 as the Trans-Pacific Strategic Economic Partnership Agreement by New Zealand, Singapore, Chile, and Brunei, gradually evolved to include countries such as Australia, Japan, and Canada over subsequent years.[410] It is arguably the first "mega-regional" agreement, which once encompassed 40 percent of world trade,[411] marking a significant milestone in global trade governance after the Doha Round faced gridlock,[412]

[409] Out of 30 RTAs that include clauses prohibits local storage requirements, over 16 RTAs provide for clauses entitled as "location of computing facilities", which generally prohibit mandatory requirements of use or locate computing facilities in signatory parties' territories as a condition for conducting business.
[410] Todd Allee & Andrew Lugg, *Who Wrote the Rules for the Trans-Pacific Partnership,* 3 RESEARCH & POLITICS 1(2016), at 2, https://www.researchgate.net/publication/305629920_Who_wrote_the_rules_for_the_Trans-Pacific_Partnership.
[411] Rebecca Howard, *Trans-Pacific Partnership Trade Deal Signed, but Years of Negotiations Still to Come,* REUTERS (Feb. 4, 2016), http://perma.cc/5DDA-2Z5B.
[412] Allee & Lugg, *supra* note 401, at 2.

doi:10.6342/NTU202402499

The TPP prohibits both local storage and processing requirements under chapter 14, the electronic commerce chapter. Article 14.13, entitled "Location of Computing Facilities" stipulates the following:[413]

> 1. The Parties recognise that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications.
>
> 2. 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.
>
> 3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective.

According to the US Trade Representative ("USTR"), Article 14.13 of the TPP is designed to guarantee that "companies will not have to build expensive and unnecessarily redundant data centres in every market they seek to serve."[414] Australia also asserts that "TPP countries cannot force businesses to build data storage centres or use local

[413] TPP, art. 14.13.
[414] *TPP Chapter Summary of Electronic Commerce*, UNITED STATES TRADE REPRESENTATIVE, https://ustr.gov/sites/default/files/TPP-ChapterSummary-Electronic-Commerce.pdf (last visited Apr. 11, 2024).

doi:10.6342/NTU202402499

computing facilities in TPP markets…providing certainty to businesses as they look to optimise investment decisions."[415] In other words, Article 14.13 is designed to grant businesses the flexibility to decide where they wish to allocate their investments for databases, thereby preventing them from building expensive and unnecessarily redundant data centres in every market they seek to serve.

Nonetheless, parties are still allowed to impose restrictions on the use or location of computing facilities to achieve a legitimate public policy objective when the requirements under TPP Article 14.13(3) are met. The language used in Article 14.13(3)(a) is similar to that of the Chapeau of GATS Article XIV and GATT 1994 Article XX. However, Article 14.13(3)(b) is different from the design of the general exception clause under both the GATT 1994 Article XX and GATS Article XIV. Both these two provisions provide an exhaustive list of policy objectives, and the legitimacy of a measure is evaluated in accordance with these objectives.[416] On the other hand, Article 14.13(3) provides an open-ended list of policy objectives, and whether an objective is legitimate shall be evaluated initially.[417] The TPP negotiators may intentionally create this "constructive ambiguity" by using ambiguously worded provisions in these politically sensitive areas to leave room for future interpretation.[418]

The wordings of Article 14.13(3)(b) suggest that the restrictions imposed by the challenging measure on the use or location of computing facilities must not be greater

---

[415] *TPP Outcomes: Trade in the Digital Age*, AUSTL. GOV. DEPT. FOREIGN AFF. & TRADE, https://www.dfat.gov.au/trade/agreements/not-yet-in-force/tpp/Pages/outcomes-trade-in-the-digital-age (last visited Apr. 11, 2024).
[416] Shin-yi Peng & Han-wei Liu, *The Legality of Data Residency Requirements: How Can the Trans-Pacific Partnership Help*, (2017), 51(2) J. WORLD TRADE 183, at 196, https://kluwerlawonline.com/journalArt./Journal+of+World+Trade/51.2/TRAD2017008.
[417] *Id.*
[418] Peng & Liu, *supra* note 407, at 196; *See* Shin-yi Peng, *Regulating New Services Through Litigation?–Electronic Commerce as a Case Study on the Evaluation of "Judicial Activism" in the WTO*, 48(6) J. WORLD TRADE 1189, at 1198 (2014).

doi:10.6342/NTU202402499

than are required to achieve the objective. Peng and Liu suggest that a TPP panel may refer to the jurisprudence of Article XX of the GATT 1994 concerning the "necessity test" to determine whether there is any other less-restrictive alternative measure reasonably available to the party[419] when their measures are inconsistent with TPP Article 14.13(2).

While TPP Article 14.13 does not contain a security exception by its own, according to TPP Article 29.2, "Nothing in this Agreement shall be construed to: (a) require a Party to furnish or allow access to any information the disclosure of which it determines to be contrary to its essential security interests; or (b) preclude a Party from applying measures that it considers necessary for the fulfilment of its obligations with respect to the maintenance or restoration of international peace or security, or the protection of its own essential security interests."[420]

The wordings of TPP Article 14.13 closely resembles that of GATS Article XIV *bis* and GATT Article XXI. However, unlike the subparagraphs of GATS Article XIV *bis* (1)(b) and GATT Article XXI (b), TPP Article 14.13 does not condition the situations under which Members may invoke security exception. In other words, TPP parties are not limited to invoking security exceptions only during wartime or in cases of international emergency.

Accordingly, TPP parties are allowed to deviate from their obligations under Article 14.13 when they consider necessary for the protection of its own essential security interests. Notably, the WTO Panel asserts that such wordings do not grant the security exception completely "self-judging" and acknowledged its justiciability.[421] In addition, while Member has the discretion to define its "essential security interests", such

[419] *Id.* at 201.
[420] TPP, art. 29.2.
[421] Panel Report, *Russia — Traffic in Transit*, ¶ 7.58.

doi:10.6342/NTU202402499

interpretation shall follow the good faith principle outlined in Article 31(1) of the Vienna Convention on the Law of Treaties,[422] ensuring the security exception is not used to circumvent GATT obligations.[423] These jurisprudences may provide insights to the TPP tribunal when determining whether TPP parties can invoke TPP Article 29.2(b) to justify their implementation of local storage requirements.

B. Comprehensive and Progressive Agreement for Trans-Pacific Partnership

The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (hereinafter "CPTPP") is a free trade agreement (hereinafter "FTA") formed by the 11 remaining Members of the proposed TPP, encompassing Canada, Australia, Brunei, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore and Vietnam, following the withdrawal of the US' signature in 2017 during the Trump Administration.[424] CPTPP largely preserves the provisions of TPP,[425] with only 20 articles modified or delayed from the extensive 8,000-page CPTPP document. Notably, none of these alterations pertained to the Electronic Commerce Chapter.[426]

Accordingly, CPTPP Article 14.13 entitled "Location of Computing Facilities", provides for identical texts which can be found in TPP Article 14.13 as follows:[427]

[422] Panel Report, *Russia — Traffic in Transit*, ¶ 7.132.
[423] *Id.* ¶ 7.133.
[424] *CPTPP: Overview and Issues for Congress*, CONGRESSIONAL RESEARCH SERVICE (June 16, 2023), https://crsreports.congress.gov/product/pdf/IF/IF12078 (last visited Apr. 11, 2024)
[425] *Id.*
[426] Xiaolian Quan, *supra* note 338, at 260.
[427] CPTPP, art. 14.13 ("1. The Parties recognise that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications. 2. 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. 3. Nothing in this Art. shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective.").

doi:10.6342/NTU202402499

1. The Parties recognise that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications.
2. 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.
3. Nothing in this Art. shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective.

Concerning the security exceptions, CPTPP Article 29.2 provides the same texts as that of TPP Article 29.2. Accordingly, CPTPP parties can still impose local storage requirements when they consider necessary for the protection of its own essential security interests.

Since the CPTPP took effect in December 2018, several additional countries, including China, have applied or shown interest in joining the CPTPP.[428] Accession to the

[428] Jeffrey J. Schott, *Which Countries are in the CPTPP and RCEP Trade Agreements and Which Want in*, PETERSON INST. INT'L ECON. (July 27, 2023), https://www.piie.com/research/piie-charts/which-countries-are-cptpp-and-rcep-trade-agreements-and-which-want.

doi:10.6342/NTU202402499

CPTPP requires a consensus among existing signatories, and applicants must satisfy every Member's concerns.[429] On September 16, 2021, China formally applied for Membership in the CPTPP after expressing its interest in joining the agreement for two years.[430] However, significant disparities between Chinese policies and CPTPP standards, particularly concerning labor practices, state-owned enterprises (SOEs), and digital trade, pose substantial challenges to Chinese accession.[431]

For instance, Article 14.13 of the CPTPP explicitly prohibits the compulsory localisation of data storage and processing by foreign companies within a country's borders. To fulfill this obligation, China may need to undertake massive legal reforms,[432] considering their current implementation of stringent local storage requirements.

C. United States-Mexico-Canada Agreement

According to the USTR, the United States-Mexico-Canada Agreement (hereinafter "USMCA") was established by the US and Mexico, with the aim of modernizing the 25-year-old NAFTA into a high-standard agreement fit for the 21st century.[433] A pivotal aspect of the USMCA is its incorporation of the new Digital Trade chapter, which "contains the strongest disciplines on digital trade of any international agreement, providing a firm foundation for the expansion of trade and investment in the innovative products and services where the US has a competitive advantage."[434]

---

[429] *Id.*
[430] *Id.*
[431] Jeffrey J. Schott, *Which Countries are in the CPTPP and RCEP Trade Agreements and Which Want in*, PETERSON INST. INT'L ECON. (July 27, 2023), https://www.piie.com/research/piie-charts/which-countries-are-cptpp-and-rcep-trade-agreements-and-which-want (last visited Apr. 11, 2024).
[432] *See* Lucy Craymer & Joe Cash, *Biggest Hurdles to China Entry into Trans-Pacific Trade Pact are Political*, REUTERS (Aug. 1, 2023), https://www.reuters.com/world/biggest-hurdles-china-entry-into-trans-pacific-trade-pact-are-political-2023-07-31/ (last visited Apr. 11, 2024).
[433] UNITED STATES-MEXICO-CANADA TRADE FACT SHEET: MODERNIZING NAFTA INTO A 21ST CENTURY TRADE AGREEMENT, https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/fact-sheets/modernizing (last visited Apr. 11, 2024).
[434] *Id.*

doi:10.6342/NTU202402499

Chapter 19 of the USMCA is the digital trade chapter, which provides for the prohibition clause on both local storage and processing requirements under Article 19.12, entitled "Location of Computing Facilities" as follows:[435]

> 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.

Notably, a significant distinction between Article 14.13 of the CPTPP and Article 19.12 of the USMCA is the absence in the latter of an emphasis on a state's right to regulate through an initial declaration.[436]

Unlike Article 14.13(3) of the CPTPP, Article 19.12 of the USMCA does not contain its own general exception clause. Instead, GATS Article XIV (a), (b) and (c) apply to USMCA Article 19.12 *mutatis mutandis*.[437]

As previously discussed in subsection A of this Chapter, Article 14.13(3) of the CPTPP provides an open-ended list of policy objectives. Whether an objective is legitimate shall be evaluated initially, resembling a looser GATT Article XX-like exception clause.[438] On the other hand, Article 19.12 of the USMCA can only be justified

[435] USMC, art. 19.12 "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."
[436] Xiaolian Quan, *supra* note 338, at 265.
[437] USMCA, art. 32.1(2) ("For the purposes of Chapter 15 (Cross-Border Trade in Services), Chapter 16 (Temporary Entry for Business Persons), Chapter 18 (Telecommunications), Chapter 19 (Digital Trade), (supra note 2) and Chapter 22 (State-Owned Enterprises and Designated Monopolies), paragraphs (a), (b), and (c) of Art. XIV of GATS are incorporated into and made part of this Agreement, mutatis mutandis. (supra note 3)")
[438] Peng & Liu, *supra* note 407, at 195.

doi:10.6342/NTU202402499

by paragraphs (a), (b), and (c) of Article XIV of GATS, indicating a stricter criterion for justifying parties' local storage requirements compared to that of the CPTPP.[439]

Accordingly, parties to USMCA cannot invoke policy objectives that are absent in paragraphs (a), (b), and (c) of GATS Article XIV to justify their measures inconsistent with Article 19.12 thereof. The USMCA thus provides for stricter general exception criteria to its "location of computing facilities" provision compared to that of the CPTPP. Such distinction may explain why the U.S. Chamber of Commerce has recognized that the "USMCA creates best-in-class rules to foster U.S. growth in the digital economy for firms of all sectors and sizes … prohibits the forced localisation of data, thereby ensuring continued growth."[440]

In terms of security exceptions, Article 32.2 which provides identical wordings as that of TPP Article 29.2,[441] can be invoked by parties to justify their deviations from USMCA Article 19.12.

D. The Digital Economy Partnership Agreement between New Zealand, Singapore, and Chile

The Digital Economy Partnership Agreement between New Zealand, Singapore, and Chile (hereinafter "DEPA") emerges as a groundbreaking initiative of digital-only trade agreement, uniting Chile, New Zealand, and Singapore as small trade-dependent countries in a forward-looking collaboration to navigate the complexities of the digital

[439] USMCA, art. 32.1(2).

[440] *U.S. Chamber Letter: USMCA Now*, U.S. CHAMBER OF COMMERCE (Oct. 1, 2019), https://www.uschamber.com/usmca (last visited Apr. 11, 2024).

[441] USMCA, art. 32.2 ("Nothing in this Agreement shall be construed to: (a) require a Party to furnish or allow access to information the disclosure of which it determines to be contrary to its essential security interests; or (b) preclude a Party from applying measures that it considers necessary for the fulfilment of its obligations with respect to the maintenance or restoration of international peace or security, or the protection of its own essential security interests.")

doi:10.6342/NTU202402499

era.[442] Signed in an entirely online virtual ceremony on June 12, 2020, the DEPA entered into force for New Zealand and Singapore on January 7, 2021.[443] As small, trade-dependent nations, these three countries share a common vision on numerous trade policy fronts.[444] With a commitment to adaptability and inclusivity, the DEPA is designed as a living agreement, poised to expand its Membership to WTO Members capable of meeting its standards.[445]

DEPA Article 4.4 entitled "Location of Computing Facilities" provides for the following texts:

> The Parties affirm their level of commitments relating to Location of Computing Facilities, for example:
>
> 1. The Parties recognise that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications.
> 2. 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.
> 3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:

[442] *The Digital Economy Partnership Agreement is a new initiative with Chile and Singapore,* NEW ZEALAND FOREIGN AFF. & TRADE, https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement-depa/overview/ (last visited on Apr. 11, 2024).
[443] *Id.*
[444] *Id.*
[445] *Id.*

doi:10.6342/NTU202402499

(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and

(b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective.

DEPA Article 4.4 contains identical language to Article 14.13 of the CPTPP, with a subtle difference concerning its opening clause stating that "the Parties affirm their level of commitments relating to location of computing facilities, in particular, but not exclusively."[446]

In terms of security exceptions, DEPA Article 13.2 provides for the same texts as that of TPP Article 29.2, allowing parties to deviate from their obligations under DEPA when they consider necessary for the protection of its own essential security interests.

On 8 June 2023, during the OECD Ministerial Council Meeting in Paris, France, Ministers from New Zealand, the Republic of Korea, Singapore, and Chile convened to acknowledge the substantial conclusion of discussions, marking a milestone as the Republic of Korea became the first nation outside the founding Members—Chile, New Zealand, and Singapore—to join the DEPA.[447] In addition, China, Canada, Costa Rica, and Peru have also expressed interest in joining and initiating formal requests and ongoing discussions with DEPA Parties.[448]

[446] DEPA, art. 4.4.
[447] *Joint press release on the Accession of the Republic of Korea to the Digital Economy Partnership Agreement*, NEW ZEALAND FOREIGN AFF. & TRADE (June 8, 2023), https://www.mfat.govt.nz/en/media-and-resources/joint-press-release-on-the-accession-of-the-republic-of-korea-to-the-digital-economy-partnership-agreement/.
[448] *Id.*

doi:10.6342/NTU202402499

E. Regional Comprehensive Economic Partnership

The Regional Comprehensive Economic Partnership (hereinafter "RCEP") emerged as a pivotal initiative to bolster trade and economic ties within the East Asia region.[449] With flourishing free trade agreements already in place between the Association of Southeast Asian Nations (ASEAN) and six partner nations including China, South Korea, Japan, India, Australia, and New Zealand, the need for a more comprehensive framework became critical.[450]

In response, leaders from 16 participating countries came together to establish RCEP, aiming to deepen economic engagement and foster regional development.[451] Launched in November 2012 during the 21st ASEAN Summit, RCEP negotiations sought to build upon existing ASEAN+1 FTAs, with the objective of creating a modern, inclusive, and mutually beneficial economic partnership agreement.[452] Encompassing trade in goods and services, investment, intellectual property, and other areas, RCEP's coverage is extensive, reflecting its ambition to address various aspects of economic cooperation.[453]

RCEP Article 12.14 entitled "Location of Computing Facilities" provides for the following texts:

> 1. The Parties recognise that each Party may have its own measures regarding the use or location of computing facilities, including

[449] *The Regional Comprehensive Economic Partnership (RCEP)*, ASS'N SOUTHEAST ASIAN NATIONS, https://asean.org/our-communities/economic-community/integration-with-global-economy/the-regional-comprehensive-economic-partnership-rcep/ (last visited on Apr. 11, 2024).
[450] *Id.*
[451] *Id.*
[452] *Id.*
[453] *Id.*

doi:10.6342/NTU202402499

requirements that seek to ensure the security and confidentiality of communications.

2. 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 Party's territory.

3. Nothing in this Article shall prevent a Party from adopting or maintaining:

(a) any measure inconsistent with paragraph 2 that it considers necessary to achieve a legitimate public policy objective, provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; or

(b) any measure that it considers necessary for the protection of its essential security interests. Such measures shall not be disputed by other Parties.

RCEP Article 12.14 contains language similar to TPP Article 14.13.[454] Notably, Article 12.14(3)(b) contains a GATT Article XXI-like language, allowing local storage requirement measures that a party considers necessary for the protection of its essential security interests, a provision absent from Article 14.13 of the CPTPP.

While security exceptions exist in TPP, CPTPP, USMCA, and DEPA, they are not specifically framed within their "location of Computing Facilities" clauses but are rather outlined in general and security exception chapters applicable throughout the agreements.

[454] RCEP, art. 12.14.

doi:10.6342/NTU202402499

In addition, RCEP Article 12.14(3)(b) explicitly states that measures that it considers necessary for the protection of its essential security interests “shall not be disputed by other Parties.”, which suggests a deliberate intent by the RCEP to afford parties full autonomy to exercise discretion in implementing measures inconsistent with RCEP Article 12.14 (2).

Given that RCEP encompasses Member countries with divergent approaches to local storage requirement regulations—ranging from stringent rules in countries like China, Indonesia, and Vietnam to policies favoring the free flow of data as seen in Singapore—it is understandable for RCEP to broaden the scope of justification for local storage requirement measures. This adjustment may cater to the policy needs of Members who impose stricter local storage requirement measures, thereby accommodating the diverse regulatory environments of parties within the RCEP framework.

II. Different Regulatory Models that Prohibit Local Storage Requirement Measures in RTAs

After examining provisions that prohibit local storage requirements in the aforementioned mega RTAs and DEA, it is notable that TPP Article 14.13 serves as a regulatory model found in other agreements. Nonetheless, while RCEP Article 12.14 closely resembles TPP Article 14.13, its security exception aligns with China's longstanding emphasis on state-centric data policies.

In navigating the evolving landscape of digital trade, distinct legal strategies have also emerged among major players, exemplified by the US, the EU, and China in their respective RTAs. As previously introduced, the USMCA prioritizes free data flow, evident in its stringent exception criteria provided for Article 19.12 thereof, showcasing a firm

doi:10.6342/NTU202402499

stance aligned with US interests and a departure from broader exception clauses seen in other agreements.

On the other hand, the EU RTAs adopts a distinctive approach to prohibiting data localisation measures in the context of cross-border data flows,[455] which sets them apart from the "location of computing facilities" provisions found in other RTAs. For instance, Article 201(1) of the Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the One Part, and the United Kingdom of Great Britain and Northern Ireland, of the Other Part (hereinafter "EU-UK TCA") only prohibits requirements leading to restrictions on cross-border data flows,[456] while providing leeway for parties to deviate from such obligations to safeguard personal data protection under certain conditions,[457] underlining the EU's commitment to privacy and data protection standards.

[455] Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the One Part, and the United Kingdom of Great Britain and Northern Ireland, of the Other Part, EU–UK, Dec. 24, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22021A0430%2801%29 (last visited Apr. 10, 2024) [hereinafter EU–UK TCA], art. 201; Free Trade Agreement between the European Union and New Zealand, EU–New Zealand, July 9, 2023, https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/new-zealand/eu-new-zealand-agreement/text-agreement_en (last visited Apr. 10, 2024) [hereinafter EU–New Zealand FTA], Chapter 12 section B art. 12.4(2); Free Trade Agreement between the EFTA States and the Republic of Moldova, June. 27, 2023, https://edit.wti.org/document/show/5dd788d0-ccd2-4392-9744-58eb6a3876a4?page=2 (last visited Apr. 10, 2024) [hereinafter EFTA–Moldova FTA], art. 5.11.

[456] EU–UK TCA, art. 201(1) ("The Parties are committed to ensuring cross-border data flows to facilitate trade in the digital economy. To that end, cross-border data flows shall not be restricted between the Parties by a Party: (a) requiring the use of computing facilities or network elements in the Party's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of a Party; (b) requiring the localisation of data in the Party's territory for storage or processing; (c) prohibiting the storage or processing in the territory of the other Party; or (d) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Parties' territory or upon localisation requirements in the Parties' territory.")

[457] EU–UK TCA, art. 202(2) ("Nothing in this Agreement shall prevent a Party from adopting or maintaining measures on the protection of personal data and privacy, including with respect to cross-border data transfers, provided that the law of the Party provides for instruments enabling transfers under conditions of general application (34) for the protection of the data transferred.")

doi:10.6342/NTU202402499

As previously discussed, China's prioritization of national security and control over data flows can be seen in the "self-judging" approach employed in RCEP Article 12.14(3)(b).

This section intends to analyze the divergent approaches of these three trade participants to prohibition clauses on data localisation measures in their RTAs, respectively.

A. The US Model

As one of the major trading nations, the US has historically championed free trade and played a leading role in promoting trade liberalization.[458] In August of 2002, the "Bipartisan Trade Promotion Authority Act of 2002" was enacted by the US Congress, representing significant advancements in the US digital trade agenda.[459] This agenda, supported by influential American business groups representing both high-tech and traditional content-producing industries,[460] aimed at minimal government intervention in regulating e-commerce and digital trade to encourage their growth. [461] This agenda reflects the US's liberal approach to digital trade, including acknowledging the importance of maintaining the free flow of information.[462] Since 2002, the US has sought

[458] *See* Juan A. Marchetti & Petros C. Mavroidis, *The Genesis of the GATS (General Agreement on Trade in Services),* 22(3) THE EUR. J. INT'L L. 689, at 690-694 (2011) (The United States took a leading role in championing the creation of the GATS, propelled by the growing economic success of its service sectors.).
[459] Sacha Wunsch-Vincent, *The Digital Trade Agenda of the U.S.: Parallel Tracks of Bilateral, Regional and Multilateral Liberalization*, 58(1) AUSSENWIRTSCHAFT 7, at 7 (2003) ("In August of last year, U.S. Congress enacted the "Bipartisan Trade Promotion Authority Act of 2002"1. Thereby it has ended an eight-year period in which the United States lacked the fast-track authority to conclude trade agreements with a simplified congressional ratification procedure. President BUSH's intention is to use the new Trade Promotion Authority (TPA) to pursue a parallel track of preferential and multilateral trade negotiations.").
[460] *Id*. at 9 ("This ambitious digital trade agenda originates from the fact that within the last couple of years a powerful alliance of American business associations that represent high-tech firms (e.g. Information Technology Industry Council) and associations that represent classical content producing firms (e.g. Motion Picture Association of America) has joined forces to voice its interests in avoiding the rise of new digital trade barriers.").
[461] *Id*. ("In its non-trade related legislation the U.S. Congress has thus followed the industry's advice that e-commerce, and digital trade of content in particular, will thrive best with a strong intellectual property regime and little government interference in other regulatory matters.").
[462] Wunsch-Vincent, at 12 ("Specific U.S. Digital Trade Policy Objectives … The importance of

doi:10.6342/NTU202402499

to advance its digital trade agenda through Free Trade Agreements[463] and has played a pivotal role in shaping the regulatory framework surrounding local storage requirement measures in several significant RTAs, including the TPP and the USMCA.

In the case of the TPP, which emerged as a landmark agreement encompassing countries spanning the Asia-Pacific region, the US involvement since 2008 marked a significant turning point. Despite the US's eventual withdrawal from the TPP, its influence on the agreement's content remained palpable, with US treaty language prominently featured throughout the agreement.[464] Article 14.13 of the TPP, titled "Location of Computing Facilities," reflects the US long-standing policy against data localisation measures. As previously introduced, this provision aims to eliminate both local storage and processing requirements that could compel companies to build costly and redundant data centres in each market they serve.

Similarly, under Chapter 19 of the USMCA, titled "Digital Trade," Article 19.12 provides for the prohibition of both local storage and processing requirement measures, preventing parties from imposing restrictions on the use or location of computing facilities as a condition for conducting business in such parties' territories.

---

maintaining free flows of information should be explicitly acknowledged.")

[463] United States–Australia Free Trade Agreement, with Annexes and Related Exchange of Letters, Austl.–U.S., May 18, 2004, 43 I.L.M. 1248 [hereinafter Australia–U.S. FTA]; Agreement Between the Government of the United States of America and the Government of the Kingdom of Bahrain on the Establishment of a Free Trade Area, Bahr.–U.S., Sep. 14, 2004, 44 I.L.M. 544 (entered into force Dec. 7, 2005); 4 I.L.M. 544 (entered into force Dec. 7, 2005). 57. United States–Chile Free Trade Agreement, Chile–U.S., Sep. 3, 2003, 114 Stat. 1526 (entered into force Jan. 1, 2004) [hereinafter U.S.–Chile FTA]; United States–Morocco Free Trade Agreement, Morocco–U.S., June 15, 2004, 44 I.L.M. 544 (entered into force Jan. 1, 2006); United States–Oman Free Trade Agreement, Oman–U.S., Jan. 18, 2006, K.A.V. 8673 (entered into force Jan. 1, 2009); United States–Peru Trade Promotion Agreement, Peru–U.S., Apr. 12, 2006, K.A.V. 9736 (entered into force Feb. 1, 2009); United States–Singapore Free Trade Agreement, Sing.–U.S., Sep. 3, 2003, 117 Stat. 948 (entered into force Jan. 1, 2004) [hereinafter U.S.–Singapore FTA]; United States–Panama Trade Promotion Agreement (entered into force Oct. 31, 2012) [hereinafter U.S.–Panama FTA]; United States–Korea Free Trade Agreement, S. Korea–U.S., June 30, 2007, 46 I.L.M. 642 (entered into force Mar. 15, 2012) [hereinafter KORUS FTA].

[464] Allee & Lugg, *supra* note 401, at 4 ("The prominence of US language in the TPP … Our analyses reveal that US treaty language is pre-eminent in the TPP, suggesting that the USA had heavy influence in writing this important new agreement.").

doi:10.6342/NTU202402499

Both the TPP and USMCA feature dedicated chapters addressing general exceptions, known respectively as TPP Chapter 29 and USMCA Chapter 32. These chapters encompass general exceptions that integrate Article XX of GATT 1994 and its interpretative notes for trade in goods, as well as Article XIV of GATS for trade in services. Nonetheless, TPP Article 14.13(3) provides looser criteria than general exceptions under the GATS to justify local storage requirement measures, which is absent under Article 19.12 of the USMCA. Article 19.12 of the USMCA did not include its own exception paragraph as Article 14.13(3) does. This distinction reflects the stricter stance of the US against local storage requirement measures.

The USMCA underscores the prioritization of free data flow over concerns for privacy protection or national cybersecurity,[465] aligning closely with the long-standing data policy stance of the US. This emphasis can be found not only in the absence of strong privacy or cybersecurity provisions thereunder but also in adding new provisions like Article 19.17, entitled "Interactive Computer Services,"[466] and Article 19.18, entitled "Open

[465] Xiaolian Quan, *supra* note 338, at 265 ("The USMCA also adds two new provisions, namely Article 19.17, Interactive Computer Services, and Article 19.18, Open Government Data. While Article 19.17 ensures that no limitation or liability shall apply on the service supplier and user, Article 19.18 requires governments to ensure transparency of government information. By enabling private stakeholder rights, and placing strong obligations on the government, the USMCA clearly favors free cross-border data flows to enable digital commerce over the objective of privacy protection or national cybersecurity.")

[466] USMCA, art. 19.17, ("1. The Parties recognize the importance of the promotion of interactive computer services, including for small and medium-sized enterprises, as vital to the growth of digital trade. 2. To that end, other than as provided in paragraph 4, no Party shall adopt or maintain measures that treat a supplier or user of an interactive computer service as an information content provider in determining liability for harms related to information stored, processed, transmitted, distributed, or made available by the service, except to the extent the supplier or user has, in whole or in part, created, or developed the information. 3. No Party shall impose liability on a supplier or user of an interactive computer service on account of: (a) any action voluntarily taken in good faith by the supplier or user to restrict access to or availability of material that is accessible or available through its supply or use of the interactive computer services and that the supplier or user considers to be harmful or objectionable; or (b) any action taken to enable or make available the technical means that enable an information content provider or other persons to restrict access to material that it considers to be harmful or objectionable. 4. Nothing in this Art. shall: (a) apply to any measure of a Party pertaining to intellectual property, including measures addressing liability for intellectual property infringement; or (b) be construed to enlarge or diminish a Party's ability to protect or enforce an intellectual property right; or (c) be construed to prevent: (i) a Party from enforcing any criminal law, or (ii) a supplier or user of an interactive computer service from complying with a specific, lawful order of a law enforcement authority. 5. This Art. is subject to Annex 19-A")

doi:10.6342/NTU202402499

Government Data."[467] These two provisions serve to bolster the rights of private stakeholders while imposing transparency obligations on governments, ultimately facilitating unfettered cross-border data flows to facilitate digital commerce.[468]

Following the establishment of the USMCA, the US further engaged in a digital trade agreement with Japan.[469] This agreement not only encompasses a general prohibition clause on local storage requirement measures[470] but also extends this prohibition to encompass financial services.[471] USMCA Article 13 prohibits signatory parties from mandating a covered financial service supplier to use or locate financial service computing facilities in their territories as a condition for conducting business, provided that their financial regulatory authorities have immediate, direct, complete, and ongoing access to information that the covered financial service supplier uses or locates in computing facilities outside the signatory parties' territories.

[467] USMCA, art. 19. 18 ("1. The Parties recognize that facilitating public access to and use of government information fosters economic and social development, competitiveness, and innovation. 2. To the extent that a Party chooses to make government information, including data, available to the public, it shall endeavor to ensure that the information is in a machine-readable and open format and can be searched, retrieved, used, reused, and redistributed. 3. The Parties shall endeavor to cooperate to identify ways in which each Party can expand access to and use of government information, including data, that the Party has made public, with a view to enhancing and generating business opportunities, especially for SMEs.")
[468] Xiaolian Quan, *supra* note 338, at 265.
[469] Japan–US DTA.
[470] Japan–US DTA, art. 12 ("1. Neither 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. 2. This Article does not apply with respect to covered financial service suppliers, which are addressed by Article 13.").
[471] Japan–US DTA, art. 13 ("1. The Parties recognize that immediate, direct, complete, and ongoing access by a Party's financial regulatory authorities to information of covered financial service suppliers, including information underlying the transactions and operations of such covered financial service suppliers, is critical to financial regulation and supervision, and recognize the need to eliminate any potential limitations on that access. 2. Neither Party shall require a covered financial service supplier to use or locate financial service computing facilities in that Party's territory as a condition for conducting business in that territory, so long as the Party's financial regulatory authorities, for regulatory and supervisory purposes, have immediate, direct, complete, and ongoing access to information processed or stored on financial service computing facilities that the covered financial service supplier uses or locates outside the territory of the Party.").

doi:10.6342/NTU202402499

Overall, the US' legal approach to data localisation measures in its RTAs reflects its long-standing policy,[472] aligning with the interests of US Big-tech firms.

B. The EU Model

The EU has long advocated for data protection and the protection of personal privacy. Its stance on data protection has evolved gradually over the years, reflecting both internal and external influences. In the 1970s, amidst the rise of data processing technologies, concerns regarding privacy and individual rights began to garner attention within the EU countries.[473] This was driven by a recognition of the need to safeguard personal information in the face of advancing technology and the potential for misuse or unauthorized access.[474] Concurrently, international instruments such as the OECD Privacy Guidelines and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe emerged, establishing a link between data protection and the promotion of trade. These instruments aimed to facilitate cross-border flows of personal data by setting minimum standards for data privacy, thereby reducing barriers to international trade.[475]

Building upon these efforts, the EU adopted Directive 95/46/EC in 1995, which marked a significant milestone in the development of data protection regulations within the EU.[476] This directive aimed to harmonize data protection laws across EU Member states and enhance the protection of individuals' personal data.[477] It emphasized the importance of fair and lawful processing of personal data, as well as the rights of

[472] US JSI Proposal.
[473] TOBIAS NAEF, *supra* note 72, at 20-22.
[474] *Id.*
[475] TOBIAS NAEF, *supra* note 72, at 22-25.
[476] *Id.* at 26.
[477] *Id.*

doi:10.6342/NTU202402499

individuals to access and rectify their data.[478] Moreover, it laid the groundwork for the establishment of a new right to data protection that is independent of the right to private life.[479] This evolution culminated in the adoption of the Charter of Fundamental Rights in 2000, which included Article 8 on the protection of personal data as a distinct and fundamental right.[480] This marked a paradigm shift in EU law, affirming data protection as a standalone right with its own set of protections and obligations, separate from the broader right to privacy.

In 2016, the GDPR, a pivotal advancement in the EU's data protection framework, has been enacted.[481] Departing from prior directives, the GDPR establishes a unified approach to data protection across the EU, leaving no room for individual Member states to enact their own rules.[482] Designed to build upon the foundation laid by Directive 95/46/EC, the GDPR maintains key legal mechanisms while introducing significant changes, including centralized adequacy assessments under the oversight of the European Commission.[483]

In addition to data protection concerns, the EU has increasingly advocated for digital sovereignty, a stance that seems to converge significantly with its strategic autonomy,[484] which entails promoting the capacity for the EU to independently determine its values and regulations as a new agenda championed by leaders like Jean-Claude Juncker, former president of the European Commission.[485] The EU emphasizes the importance of building

[478] *Id.*
[479] *Id.*
[480] TOBIAS NAEF, *supra* note 72, at 28.
[481] *See* GDPR.
[482] TOBIAS NAEF, *supra* note 72, at 127.
[483] *Id.*
[484] Elaine Fahey, *Does the EU's Digital Sovereignty Promote Localisation in Its Model Digital Trade Clauses*, 8(2) EUR. PAPERS 503, at 504 (2023), https://www.europeanpapers.eu/en/europeanforum/does-eu-digital-sovereignty-promote-localisation.
[485] *Id*; *President Jean-Claude Juncker's State of the Union Address 2018*, EUR. COMM'N (Sept. 12, 2018), https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_18_5808 (last visited Apr. 11, 2024).

doi:10.6342/NTU202402499

a truly digital single market, enabling the bloc to define its own rules and make autonomous technological choices. Central to this vision is the development and deployment of strategic digital capacities and infrastructure, ensuring the EU's ability to shape global rules and standards.[486]

Following the EU's implementation of the GDPR, the European Commission has crafted notable model "horizontal" clauses regarding cross-border data flows and personal data protection within EU trade and investment agreements.[487] The clauses generally state that the EU favors the movement of data across borders to enhance trade and will refrain from limiting these flows by mandating data storage within the other party's territory.[488]

---

[486] European Council Conclusions, Oct. 1-2, 2020, EUCO 13/20 (2020), ¶ 7, https://data.consilium.europa.eu/doc/document/ST-13-2020-INIT/en/pdf ("To be digitally sovereign, the EU must build a truly digital single market, reinforce its ability to define its own rules, to make autonomous technological choices, and to develop and deploy strategic digital capacities and infrastructure. At the international level, the EU will leverage its tools and regulatory powers to help shape global rules and standards. The EU will remain open to all companies complying with European rules and standards. Digital development must safeguard our values, fundamental rights and security, and be socially balanced. Such a human-centred approach will increase the attractiveness of the European model.").

[487] *Horizontal provisions for cross-border data flows and for personal data protection*, EUROPEAN COMMISSION NEWSROOM (May 18, 2018), https://ec.europa.eu/newsroom/just/items/627665 (last visited Apr. 12, 2024).

[488] *Id.* art. A ("1. The Parties are committed to ensuring cross-border data flows to facilitate trade in the digital economy. To that end, cross-border data flows shall not be restricted between the Parties by: (i) requiring the use of computing facilities or network elements in the Party's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of a Party; (ii) requiring the localisation of data in the Party's territory for storage or processing;(iii) prohibiting storage or processing in the territory of the other Party; (iv) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Parties' territory or upon localisation requirements in the Parties' territory. 2. The Parties shall keep the implementation of this provision under review and assess its functioning in 3 years following the entry into force of this Agreement. A Party may at any time propose to the other Party to review the list of restrictions listed in the preceding paragraph. Such request shall be accorded sympathetic consideration."); art. B ("Protection of personal data and privacy 1. Each Party recognises that the protection of personal data and privacy is a fundamental right and that high standards in this regard contribute to trust in the digital economy and to the development of trade. 2. Each Party may adopt and maintain the safeguards it deems appropriate to ensure the protection of personal data and privacy, including through the adoption and application of rules for the cross-border transfer of personal data. Nothing in this agreement shall affect the protection of personal data and privacy afforded by the Parties' respective safeguards. 3. For the purposes of this agreement, "personal data" means any information relating to an identified or identifiable natural person. 4. For greater certainty, the Investment Court System does not apply to the provisions in Art. A and B.").

doi:10.6342/NTU202402499

These model clauses primarily aimed at constraining restrictions on cross-border data transfers, without enforcing a general prohibition on both local storage and processing requirements. This approach differs from the "location of computing facilities" provisions observed in agreements such as the CPTPP, USMCA, and China's RCEP implementation model, which prohibit both local storage and processing requirements.

An illustration of such model clauses can be found in Article 201 of the Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the One Part, and the United Kingdom of Great Britain and Northern Ireland, of the Other Part (hereinafter "EU-UK TCA"), Chapter 12, section B, Article 12.4(2) of Free Trade Agreement between the European Union and New Zealand, EU-New Zealand EU-UK Trade and Cooperation Agreement (hereinafter "EU-New Zealand FTA"), and Article 5.11 of the Free Trade Agreement between the EFTA States and the Republic of Moldova (hereinafter "EFTA-Moldova FTA").[489]

For instance, Title III Digital Trade, Chapter 2 DATA FLOWS AND PERSONAL DATA PROTECTION of the EU-UK Trade and Cooperation Agreement, focuses on data flows and personal data protection, with Article 201(1) explicitly addressing cross-border data flows. Article 201(1) prohibits any Party from restricting cross-border data flows by mandating the use of specific computing facilities or network elements for processing, localizing data within its territory, prohibiting storage or processing in the territory of the other Party, or making cross-border data transfer contingent upon certain requirements.[490]

[489] EU–UK TCA, art. 202; EU–New Zealand FTA, Chapter 12 section B art. 12.4(2); EFTA–Moldova FTA, art. 5.11.

[490] EU–UK TCA, art. 201 ("1. The Parties are committed to ensuring cross-border data flows to facilitate trade in the digital economy. To that end, cross-border data flows shall not be restricted between the Parties by a Party: (a) requiring the use of computing facilities or network elements in the Party's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of a Party; (b) requiring the localisation of data in the Party's territory for storage or processing; (c) prohibiting the storage or processing in the territory of the other Party; or (d) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Parties'

doi:10.6342/NTU202402499

This provision is identical to Article A of the model "Horizontal provisions on cross-border data flows and personal data protection", developed by the European Commission in the wake of the introduction of the EU's GDPR. This is also the first time the EU has agreed on provisions for data flow in a free trade agreement.[491]

Notably, Article 201:1 differs from provisions titled "location of computing facilities" prohibiting local storage requirement measures in other agreements,[492] as it prohibits local storage requirement measures only when they restrict cross-border data flows between the parties. In contrast, provisions titled "location of computing facilities" under other RTAs generally prohibit local storage requirement measures as a condition for conducting business in such parties' territories, irrespective of their impact on cross-border data transfers. Moreover, these agreements differentiate between local storage requirement measures and cross-border data transfer as distinct legal subjects, each governed by separate provisions.[493]

Article 202 emphasizes the recognition of individuals' rights to the protection of personal data and privacy, highlighting the importance of maintaining high standards in

territory or upon localisation requirements in the Parties' territory. 2. The Parties shall keep the implementation of this provision under review and assess its functioning within three years of the date of entry into force of this Agreement. A Party may at any time propose to the other Party to review the list of restrictions listed in paragraph 1. Such a request shall be accorded sympathetic consideration.").

[491] *UK-EU Trade and Cooperation Agreement Summary*, GOV. UK, at 15, https://assets.publishing.service.gov.uk/media/602cf3dbd3bf7f031ce1360e/TCA_SUMMARY_PDF_V1-.pdf (last visited Apr. 12, 2024).

[492] Japan–Mongolia FTA, art. 9.10; TPP, art. 14.13;SAFTA art. 24 Location of Computing Facilities; Singapore–Sri Lanka FTA, art. 9.10 Location of Computing Facilities; Australia–Peru FTA, art. 13.12 Location of Computing Facilities; CPTPP, art. 14.13: Location of Computing Facilities; USMCA, art. 19.12 Location of Computing Facilities; ASEAN E-commerce Agreement, art. 7; Australia–Indonesia CEPA, art. 13.12: Location of Computing Facilities; Australia–Hong Kong FTA art. 11.8 Location of Computing Facilities; Japan–US DTA, art. 12 Location of Computing Facilities; ASDEA, art. 24 Location of Computing Facilities; RCEP, art. 12.14: Location of Computing Facilities; Australia–UK FTA, art. 14.11 Location of Computing Facilities; Singapore–UK DEA, art. 8.61-G Location of Computing Facilities; New Zealand–UK FTA, art. 15.15 Location of Computing Facilities; UK–Ukraine Digital Trade Agreement, art. 132-L Location of Computing Facilities; Korea–Singapore DEA, art. 14.15.

[493] *See e.g.*, DEPA, art. 4.3 & 4.4; CPTPP, art. 14.13 & 14.14; USMCA, art. 19.11 & 19.22; RCEP, art. 12.14 & 12.15.

doi:10.6342/NTU202402499

this regard to foster trust in the digital economy and facilitate trade development.[494] Article 202:2 further acknowledges the need for each party to adopt or maintain measures to protect personal data and privacy, serving as a justification exception for any deviation from the agreement, including regulations concerning cross-border data transfers.[495] In other words, parties may deviate from Article 201 to protect personal data and privacy as long as their laws restricting cross-border data transfers still provide for instruments enabling transfers under conditions of general application.

In general, the EU's approach to data localization measures within their RTAs mainly prohibits local processing requirements and restrictions on cross-border data transfers, which can impede the free flow of data. Accordingly, local storage requirements that merely request a copy of data to be stored locally without mandating exclusive storage in specific regions are not prohibited by the EU model clause on cross-border data flows.

C. The China Model

China has consistently advocated for state-centric digital sovereignty[496] and imposed various local storage requirements. Nonetheless, China's participation in the RCEP could potentially reflect its acceptance of specific legal approaches regarding the prohibition of local storage requirements in its future RTAs. The RCEP's e-commerce chapter is built on the CPTPP's framework. However, regarding the prohibition of local storage

[494] EU–UK TCA, art. 202 Protection of personal data and privacy ("1. Each Party recognises that individuals have a right to the protection of personal data and privacy and that high standards in this regard contribute to trust in the digital economy and to the development of trade. 2. Nothing in this Agreement shall prevent a Party from adopting or maintaining measures on the protection of personal data and privacy, including with respect to cross-border data transfers, provided that the law of the Party provides for instruments enabling transfers under conditions of general application (supra note 1) for the protection of the data transferred. 3. Each Party shall inform the other Party about any measure referred to in paragraph 2 that it adopts or maintains. supra note 1 For greater certainty, "conditions of general application" refer to conditions formulated in objective terms that apply horizontally to an unidentified number of economic operators and thus cover a range of situations and cases.").

[495] *Id.*

[496] China JSI Proposal.

doi:10.6342/NTU202402499

requirements, the RCEP modifies its language to provide Member states with the flexibility to implement restrictive measures as they see fit.

Specifically, RCEP's Article 12.14 closely resembles the initial three paragraphs of Article 14.13 in the CPTPP. However, a notable departure arises with the inclusion of footnote 12 in RCEP's provision 12.14(3)(a), stating "For the purposes of this subparagraph, the Parties affirm that the necessity behind the implementation of such legitimate public policy shall be decided by the implementing Party." Essentially, this implies that the legitimacy of any public policy mandating a firm to locate computing facilities within a Member state is subject to self-assessment. In other words, any policy can be deemed legitimate solely based on a Party's assertion. In addition, Article 12.14(3)(b) provides that "any measure that it considers necessary for the protection of its essential security interests. Such measures shall not be disputed by other Parties.", reinforcing Member states' sovereignty over local storage requirement measures.

Unlike the CPTPP, which offers provisions limiting restrictions based on legitimate public policy objectives, the RCEP's approach grants Member states broader discretion in imposing measures without stringent limitations. Additionally, according to Article 12.17(3) of the RCEP, the entire Chapter 12 is not subject to the dispute settlement procedures outlined in Chapter 19, rendering Article 12.14 with a soft law-like status.

So far, China has not committed to any mandatory clause prohibiting local storage requirement measures in any RTAs, which aligns with its national policy of pro-local storage requirement approach. However, on 16 September 2021, China officially informed New Zealand of its desire to initiate talks regarding its accession to the CPTPP.[497] He Yadong, a Ministry of Commerce spokesperson, expressed China's

[497] *4. Applications to the CPTPP: the United Kingdom, China, Taiwan and South Korea*, PARLIAMENT OF

doi:10.6342/NTU202402499

assurance of meeting the stringent standards outlined by the CPTPP during a press conference in 2024.[498] If China's application to join the CPTPP is accepted, China will then be obliged to ensure its local storage requirements comply with Article 14.13 thereof.

III. The Convergence and Divergence of "Location of Computing Facilities" Provisions.

As noted above, the EU model clause of cross-border data does not generally prohibit local storage requirements unless they lead to restrictions on the free flow of data. Therefore, the primary focus of the EU's approach is to tackle issues arising from data flow constraints rather than the trade implications of mandating the use of local computing facilities. On the other hand, "location of computing facilities" provisions in RTAs and DEAs generally prohibit local storage and processing requirements that compel the use of local computing facilities as a condition of conducting businesses. These provisions aim to reduce compliance costs by avoiding the need to build expensive and redundant data centres in every market they serve.[499] Accordingly, "location of computing facilities." provisions are more relevant for addressing the trade impact resulting from local storage requirements.

This section thus focuses on examining the convergent and divergent aspects of such provisions in various RTAs and DEAs, with the aim of providing regulatory insights to

---

AUST'L, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Foreign_Affairs_Defence_and_Trade/CPTPPMembership/Report/section?id=committees%2Freportjnt%2F024826%2F78218 (last visited Apr. 12, 2024).

[498] *China to speed up accession to CPTPP,* CHINA INT'L IMPORT EXPO (Mar. 22, 2024), https://english.www.gov.cn/news/202403/22/content_WS65fcddf2c6d0868f4e8e555c.html (last visited Apr. 12, 2024).

[499] *TPP Chapter Summary of Electronic Commerce*, UNITED STATES TRADE REPRESENTATIVE, https://ustr.gov/sites/default/files/TPP-ChapterSummary-Electronic-Commerce.pdf (last visited Apr. 11, 2024).

doi:10.6342/NTU202402499

the WTO legal framework on mitigating the adverse trade effects of local storage requirements.

A. The Nature of "Location of Computing Facilities" Provisions.

Local storage requirements mandate data storage within designated geographic boundaries. Such measures may necessitate either physical storage in paper forms or digital storage in local data centres. Notably, RTAs that prohibit local storage requirement measures, commonly referred to as "Location of Computing Facilities" provisions ("the LCF provisions"), generally prohibit the use or location of computing facilities as a condition to conduct business within parties' territory. In other words, requirements for local storage mandating physical storage but not necessarily involving the use of computing facilities do not fall under the LCF provisions outlined in these RTAs. Accordingly, local storage requirements mandating entities to retain a physical copy of certain data are not prohibited under the LCF provisions.

This is probably because the LCF provisions are prevalently provided for within the E-Commerce or Digital Trade Chapter.[500] The normative rationale behind the LCF provisions centers around the prevention of investment in expensive and unnecessarily redundant data centres,[501] thus ensuring businesses' flexibility in choosing the location of

[500] Japan–Mongolia FTA, art. 9.10; TPP, art. 14.13;SAFTA art. 24 Location of Computing Facilities; Singapore–Sri Lanka FTA, art. 9.10 Location of Computing Facilities; Australia–Peru FTA, art. 13.12 Location of Computing Facilities; CPTPP, art. 14.13: Location of Computing Facilities; USMCA, art. 19.12 Location of Computing Facilities; ASEAN E-commerce Agreement, art. 7; Australia–Indonesia CEPA, art. 13.12: Location of Computing Facilities; Australia–Hong Kong FTA art. 11.8 Location of Computing Facilities; Japan–US DTA, art. 12 Location of Computing Facilities; ASDEA, art. 24 Location of Computing Facilities; RCEP, art. 12.14: Location of Computing Facilities; Australia–UK FTA, art. 14.11 Location of Computing Facilities; Singapore–UK DEA, art. 8.61-G Location of Computing Facilities; New Zealand–UK FTA, art. 15.15 Location of Computing Facilities; UK–Ukraine Digital Trade Agreement, art. 132-L Location of Computing Facilities; Korea–Singapore DEA, art. 14.15.

[501] *Chapter Summary of Electronic Commerce*, UNITED STATES TRADE REPRESENTATIVE, https://ustr.gov/sites/default/files/TPP-ChapterSummary-Electronic-Commerce.pdf (last visited Apr. 11, 2024).

doi:10.6342/NTU202402499

their data centres.[502] Accordingly, traditional data retention laws, such as those mandating companies to preserve physical copies of their financial statements for a certain period,[503] are not the types of regulations targeted for prohibition by the LCF provisions.

This regulatory trend suggests that countries are primarily focused on addressing the adverse trade impact arising from local storage mandates within the digital landscape. Subsequent subsections further analyze the definition, scope, obligations, and exceptions of the LCF provisions.

B. The Definition of "Computing Facilities"

In RTAs that provide for the LCF provisions, the term "computing facilities" is prevalently defined as "computer servers and storage devices for processing or storing information for commercial use."[504] However, distinctions can still be found in certain RTAs that specify exclusions to this definition, with the intention of exempting certain sectors from the application of provisions related to the "Location of Computing Facilities." For instance, Article 9.1(a) of Singapore Sri Lanka FTA excludes facilities used for the supply of public telecommunications services from the definition of "computing facilities",[505] while Chapter 14, Article 1(b) of the Australia-Singapore

[502] *TPP Outcomes: Trade in the Digital Age*, AUSTL. GOV. DEPT. FOREIGN AFF. & TRADE, https://www.dfat.gov.au/trade/agreements/not-yet-in-force/tpp/Pages/outcomes-trade-in-the-digital-age (last visited Apr. 11, 2024).
[503] MATTHIAS BAUER ET AL., *supra* note 43, at 6 ("In Sweden, documents such as a company's annual reports, balance sheets and annual financial reports must be physically stored in Sweden for a period of seven years.").
[504] TPP, art. 14.1; Chile–Uruguay FTA art. 8.1; SAFTA art. 14.1; Argentina–Chile FTA art. 11.1; Australia–Peru FTA art. 13.1; CPTPP art. 14.1; Brazil–Chile FTA art. 10.1; ASEAN E-commerce Agreement art. 1; Australia–Indonesia CEPA, art. 13.1; Australia–Hong Kong FTA art. 11.2; Japan–US DTA, art. 1; DEPA, art. 4.1; RCEP art. 12.1; New Zealand–UK FTA, art. 15.1; UK–Ukraine Digital Trade Agreement, art. 131.
[505] *See e.g.*, Singapore–Sri Lanka FTA, art. 9.1 Definitions ("For purposes of this Chapter: (a) "computing facilities" means computer servers and storage devices for processing or storing information for commercial use, and does not include facilities used for the supply of public telecommunications services").

doi:10.6342/NTU202402499

Digital Economy Agreement ("ASDEA") excludes computer servers or storage devices used to access financial market infrastructures.[506]

While there is no uniform definition of "computing facilities" across all RTAs, the common definition suggests that countries implementing the LCF provisions aim to mitigate adverse effects on the commercial market caused by requirements mandating local computer servers and storage devices used in processing or storing information.

C. The Application Scope of the LCF Provisions

Including the LCF provisions within RTAs reflects a growing recognition of the importance of prohibiting local storage requirement measures. However, the scope of these provisions varies across different agreements.

The LCF provisions are predominantly governed within the digital trade or e-commerce chapters of the RTAs,[507] or within the DEAs.[508] The general scope of these digital trade and e-commerce chapters and DEAs commonly excludes government procurement[509] and measures related to information held or processed by or on behalf of a party.[510] Notably, some RTAs do not entirely exempt measures related to information

[506] *See e.g.*, ASDEA Chapter 14 (Digital Economy), art. 1 Definitions ("For the purposes of this Chapter: (b) "computing facilities" means computer servers and storage devices for processing or storing information for commercial use but does not include computer servers or storage devices of or used to access financial market infrastructures").
[507] *See e.g.*, Japan–Mongolia FTA, Chapter 9 Electronic Commerce, art. 9.10; TPP, Chapter 14 Electronic Commerce, art. 14.13; CPTPP, Chapter 14 Electronic Commerce, art. 14.13; USMCA, Chapter 19 Digital Trade, art. 19.12.
[508] See ASEAN E-commerce Agreement Art. 7(6); DEPA Art. 4.4; Australia Singapore Digital Economy Agreement (ASDEA) Art. 24; Singapore–UK DEA Art. 8.61-G.
[509] *See e.g.*, TPP, art. 14.2 (3)(a); SAFTA, art. 14.2(2)(a), Singapore–Sri Lanka FTA, art. 9.2(5); Australia-Peru FTA, art. 13.2(3)(1); CPTPP, art. 14.2(3)(a); USMCA, art. 19.2(3)(a); ASEAN E-commerce Agreement Art. 3(2); Australia–Indonesia CEPA, art. 13.2(3); Australia–Hong Kong FTA, art. 11.1(3); Japan–US DTA, art. 2(2)(a); ASDEA, art. 2(2)(a), DEPA, art. 1.1(2)(a); RCEP, art. 12.3(2), Australia–UK FTA, art. 14.2(2)(b); Singapore–UK DEA, art. 8.58(4)(b), New Zealand–UK FTA, art. 15.3(2)(b).
[510] *See e.g.*, TPP, art. 14.2 (3)(b); SAFTA, art. 14.2(2)(b); Singapore–Sri Lanka FTA, art. 9.2(5)(b); Australia–Peru FTA, art. 13.2(3)(2); CPTPP, art. 14.2 (3)(b); USMCA, art. 19.2(3)(b); Australia–Indonesia CEPA art. 13.2(3); Australia–Hong Kong FTA art. 11.1(3); Japan–US DTA. art. 2(2)(d); ASDEA, art. 2(2)(b); DEPA, art. 1.1(2)(d); RCEP, art. 12.3(3); Chile–Paraguay FTA, art. 7.2(2)(c), Singapore–UK DEA, art. 8.58(4)(c).

doi:10.6342/NTU202402499

held or processed by or on behalf of a party from the entire digital trade or e-commerce chapters. Instead, they only exempt them from the application of the LCF provisions.[511]

In addition, sectors associated with either sensitive data or matters of national interest are commonly exempted from the scope of the LCF provisions. For instance, RTAs like the TPP,[512] CPTPP,[513] Australia-Indonesia CEPA,[514] and Japan-US Digital Trade Agreement (DTA),[515] exclude financial sectors or institutions from the application of the LCF provisions. This exemption is usually achieved by defining financial service suppliers or investors as not falling under the category of "covered persons" subject to the LCF provisions. Furthermore, exclusions of some RTAs extend to credit information or related personal data.[516]

D. The General Principles of the LCF Provisions

[511] Australia–UK FTA Art. 14.2(3), New Zealand–UK FTA Art. 15.3(3).
[512] TPP, art. 14.1 Definitions ("covered person means: (a) a covered investment as defined in Art. 9.1 (Definitions); (b) an investor of a Party as defined in Art. 9.1 (Definitions), but does not include an investor in a financial institution; or (c) a service supplier of a Party as defined in Art. 10.1 (Definitions), but does not include a "financial institution" or a "cross-border financial service supplier of a Party" as defined in Art. 11.1 (Definitions).
[513] CPTPP, art. 14.1 Definitions ("covered person means: (a) a covered investment as defined in Art. 9.1 (Definitions); (b) an investor of a Party as defined in Art. 9.1 (Definitions), but does not include an investor in a financial institution; or (c) a service supplier of a Party as defined in Art. 10.1 (Definitions), but does not include a "financial institution" or a "cross-border financial service supplier of a Party" as defined in Art. 11.1 (Definitions).
[514] Australia–Indonesia CEPA, art. 13.1: Definitions ("For the purposes of this Chapter: computing facilities means computer servers and storage devices for processing or storing information for commercial use; covered person means: 1.a service supplier of the other Party within the meaning of Chapter 9 (Trade in Services);2.an investor of a Party as defined in Chapter 14 (Investment), excluding an investor in a financial institution; or 3.a covered investment as defined in Chapter 1 (Initial Provisions and General Definitions), but does not include a "financial institution" or a "financial service supplier" as defined in Chapter 10 (Financial Services), or a credit reporting body").
[515] Japan–US DTA, art. 1 Definitions ("For the purposes of this Agreement … (c) "covered enterprise" means, with respect to a Party, an enterprise in its territory, owned or controlled, directly or indirectly, by an investor of the other Party, in existence as of the date of entry into force of this Agreement or established, acquired, or expanded thereafter; (d) "covered financial service supplier" means: (i) a financial institution of the other Party; or (ii) a financial service supplier of the other Party, other than a financial institution of the other Party, that is subject to regulation, supervision, and licensing, authorization, or registration by a financial regulatory authority of the Party; (e) "covered person" means: (i) covered enterprise; or (ii) person of the other Party.").
[516] ASDEA, art. 2(4); Australia–Hong Kong FTA, art. 11.1(4); Australia–Indonesia CEPA, art. 13.1; SAFTA, art. 14.2(4).

doi:10.6342/NTU202402499

The principles provided by the LCF provisions in RTAs generally reflect a shared recognition among signatory parties of the importance of prohibiting a "covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory."[517] Analyzing the LCF provisions of multiple RTAs and DEAs[518] reveals several commonalities in their obligations.

Firstly, the majority of the LCF provisions acknowledge the regulatory autonomy of each party concerning the use of computing facilities, usually stating in the first paragraph "the Parties recognise that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications."[519] This acknowledgment reflects the need for flexibility in regulatory frameworks to accommodate varying national interests and priorities related to local storage requirement measures.

Secondly, the LCF provisions generally prohibit parties from mandating covered persons, including service suppliers, investors, or juridical persons, to use or locate computing facilities within their territory as a condition for conducting business. This prohibition ensures that regulations mandating the usage or location of the computing facilities within a signatory party's territory will not hinder a covered person's ability to

[517] Japan–Mongolia FTA, art. 9.10; TPP, art. 14.13; SAFTA art. 24 Location of Computing Facilities; Singapore–Sri Lanka FTA, art. 9.10 Location of Computing Facilities; Australia–Peru FTA, art. 13.12 Location of Computing Facilities; CPTPP, art. 14.13: Location of Computing Facilities; USMCA, art. 19.12 Location of Computing Facilities; ASEAN E-commerce Agreement, art. 7; Australia–Indonesia CEPA, art. 13.12: Location of Computing Facilities; Australia–Hong Kong FTA art. 11.8 Location of Computing Facilities; Japan–US DTA, art. 12 Location of Computing Facilities; ASDEA, art. 24 Location of Computing Facilities; RCEP, art. 12.14: Location of Computing Facilities; Australia–UK FTA, art. 14.11 Location of Computing Facilities; Singapore–UK DEA, art. 8.61-G Location of Computing Facilities; New Zealand–UK FTA, art. 15.15 Location of Computing Facilities; UK–Ukraine Digital Trade Agreement, art. 132-L Location of Computing Facilities; Korea–Singapore DEA, art. 14.15.

[518] *Id.*

[519] *See e.g.*, TPP, art. 14.13(1); SAFTA, art. 24(1); Singapore–Sri Lanka FTA, art. 9.10(1); Australia–Peru FTA, art. 13.12(1); CPTPP, art. 14.13(1); ASEAN E-commerce Agreement, art. 7(6)(a); Australia–Indonesia CEPA, art. 13.12(1); Australia–Hong Kong FTA, art. 11.8(1); ASDEA, art. 24(1); RCEP, art. 12.14(1); Australia–UK FTA, art. 14.11(1); Singapore–UK DEA, art. 8.61-G(1); New Zealand–UK FTA, art. 15.15(1); UK–Ukraine Digital Trade Agreement, art. 132-L(1).

doi:10.6342/NTU202402499

conduct businesses where such regulations are imposed. Accordingly, if a covered person is required to comply with any signatory party's local storage requirement rules as a condition for conducting business, then such requirement is prohibited under the LCF provisions.

E. The Exceptions of the LCF Provisions

The E-Commerce Chapter or Digital Trade Chapters, where the LCF provisions can be found, are typically only subject to GATS Article XIV *mutatis mutandis* under these RTAs' general exception clauses or chapters.[520] However, the absence of explicit application of GATT Article XX to the LCF provisions does not necessarily imply that signatory countries do not perceive local storage requirement measures as problems in trade in goods. While local storage requirement measures may affect both trade in services and trade in goods, the specific regulatory treatment within RTAs may reflect a prioritization of addressing barriers to trade in services resulting from data localisation measures within the e-commerce framework. Besides, most LCF provisions embody their own exception paragraph, typically encompassing a GATS Article XIV-like language, but usually with looser criteria.

GATS Article XIV provides an exhaustive list of policy objectives, and the legitimacy of a measure is evaluated in accordance with these objectives. On the other hand, exceptions such as Article 9.10(2) of the Japan-Mongolia FTA provide an open-ended list of policy objectives, and whether an objective is legitimate shall be evaluated initially.[521]

---

[520] *See e.g.* TPP Art. 29.1(3) ("3. For the purposes of Chapter 10 (Cross-Border Trade in Services), Chapter 12 (Temporary Entry for Business Persons), Chapter 13 (Telecommunications), Chapter 14 (Electronic Commerce)Footnote2 and Chapter 17 (State-Owned Enterprises and Designated Monopolies), paragraphs (a), (b) and (c) of Art. XIV of GATS are incorporated into and made part of this Agreement, mutatis mutandis.(Footnote3) The Parties understand that the measures referred to in Art. XIV(b) of GATS include environmental measures necessary to protect human, animal or plant life or health.").

[521] Japan–Mongolia FTA, art. 9.10(2) ("Notwithstanding paragraph 1, nothing in this Art. shall be construed to prevent a party from adopting or maintaining measures affecting the use or location of computing

doi:10.6342/NTU202402499

This regulatory design was further adopted in TPP Article 14.13(3)[522] and becomes prevalent across numerous other LCF provisions.[523] These exception clauses allow signatory parties to justify measures deviating from the LCF provisions to pursue legitimate public policy objectives not explicitly outlined in GATS Article XIV.

Some LCF provisions further include wording akin to GATS XIV *bis*, particularly regarding essential security interests. For instance, in the Australia-Indonesia CEPA Article 13.12(3)(b), it is stated that "Nothing in this Article shall prevent a Party from adopting or maintaining: (b) any measure that it considers necessary for the protection of its essential security interests." Similar language can also be observed in RCEP Article 12.14(3)(b).[524] However, only few LCF provisions include their own security exceptions. For instance, among the various FTAs in which Australia participates,[525] only the Australia-Indonesia Comprehensive Economic Partnership Agreement (CEPA) Article 13.12(3) includes a provision akin to GATS Article XIV *bis*.

Nonetheless, even if the LCF provisions themselves do not include security exceptions, RTAs and DEAs typically incorporate security exceptions clauses. These

facilities necessary to achieve a legitimate public policy objective, provided that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade.").

[522] TPP, art. 14.13(3) ("Nothing in this Art. shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective.").

[523] *See e.g.*, Chile–Uruguay FTA, art. 8.11(3); SAFTA, Chapter 14 art. 24 (3); CPTPP, art. 14.13(3); Australia–Hong Kong FTA, art. 11.8(3); Australia–Peru FTA, art. 13.12(3); ASDEA, art. 24(3); Australia–UK FTA art. 14.11(3); Singapore–UK DEA art. 8.61-G (3); New Zealand–UK FTA, art. 15.15(3); UK–Ukraine Digital Trade Agreement Art. 132-L (3).

[524] RCEP, art. 12.14(3) ("Nothing in this Art. shall prevent a Party from adopting or maintaining: (a) measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; or (b) any measure that it considers necessary for the protection of its essential security interests.").

[525] SAFTA, Chapter 14, art. 24; CPTPP, art. 14.13; Australia–Indonesia CEPA, art. 13.12; Australia–Hong Kong FTA, art. 11.8; Australia–Peru FTA, art. 13.12; ASDEA, art. 24; Australia–UK FTA, art. 14.11.

doi:10.6342/NTU202402499

security exceptions allow parties to deviate from their obligations under RTAs and DEAs when they consider necessary for the protection of their essential security interests.[526]

IV. Conclusion

The regulatory landscape of prohibition clauses related to data localisation measures appears similar as we delve into various RTAs and DEAs. The emergence of the LCF provisions underscores the increasing significance of data in international trade and the imperative to address the adverse trade impact resulting from local storage and processing requirements in the digital framework.

In general, the regulatory models of prohibition clauses concerning data localisation measures from the US, the EU, and the China, mainly reflect their stances as outlined in their proposals to the JSI. While the LCF provisions in agreements like CPTPP, USMCA, and DEPA differ in their general exceptions' design, they collectively embody the US long-standing spirit which prohibits the requirements that mandate the use or location of computing facilities in signatory parties' territory as a condition for conducting business.

Conversely, the EU model takes a distinctive stance aiming to liberalize cross-border data flows. The EU approach generally permits local storage requirements unless they

[526] SAFTA, Chapter 14, art. 9 ("this Chapter shall be subject to the general and security exceptions listed in Articles 18 (General Exceptions) and 19 (Security Exceptions) of Chapter 7 (Trade in Services)."); CPTPP, art. 29.2 ("Nothing in this Agreement shall be construed to: (a) require a Party to furnish or allow access to any information the disclosure of which it determines to be contrary to its essential security interests; or (b) preclude a Party from applying measures that it considers necessary for the fulfilment of its obligations with respect to the maintenance or restoration of international peace or security, or the protection of its own essential security interests."); TPP, art. 29.2 ("Nothing in this Agreement shall be construed to: (a) require a Party to furnish or allow access to any information the disclosure of which it determines to be contrary to its essential security interests; or (b) preclude a Party from applying measures that it considers necessary for the fulfilment of its obligations with respect to the maintenance or restoration of international peace or security, or the protection of its own essential security interests."); DEPA, art. 13.2 ("Nothing in this Agreement shall be construed to: (a) require a Party to furnish or allow access to any information the disclosure of which it determines to be contrary to its essential security interests; or (b) preclude a Party from applying measures that it considers necessary for the fulfilment of its obligations with respect to the maintenance or restoration of international peace or security, or the protection of its own essential security interests.").

doi:10.6342/NTU202402499

impede cross-border data transfers, and allows personal data protection to serve as an exception to restrict cross-border data transfers.

China's approach is exemplified by the RCEP Article 12.14, which holds a soft-law-like status given that the entire RCEP E-commerce Chapter falls outside the dispute settlement mechanism. However, ongoing discussions regarding China's potential accession to the CPTPP suggest that the CPTPP model could potentially influence China's standards for local storage requirement rules in future trade agreements.

Although local storage requirement measures include physical or digital storage requirements, the LCF provisions merely aim to prohibit measures mandating digital storage. Despite commonalities in prohibiting mandatory use or location of computing facilities, the scope and exceptions of these provisions differ. These divergences reflect the diverse interests and priorities of participating nations.

Based on these insights, the upcoming chapter seeks to address the following questions: (i) Should local storage requirement requirements be prohibited directly under the WTO? and (ii) How should the WTO prohibit local storage requirement requirements?

doi:10.6342/NTU202402499

CHAPTER FIVE

LOCAL STORAGE REQUIREMENTS AND THE WTO?

While GATS does not explicitly prohibit local storage requirements, some WTO Members have already advocated for trade rules that prohibit these requirements during the discussions of JSI.[527] Furthermore, as Chapter Four has discussed, the number of LCF provisions has gradually increased in RTAs and DEAs since 2014. These LCF provisions are usually designed to eliminate both local storage and processing requirements that may mandate companies to invest in data centres in markets where they seek to serve.

Consequently, this Chapter discusses whether local storage requirements should be regulated directly under the WTO law in Sections I and II. After explaining why local storage requirements should be regulated within the context of e-commerce, this thesis proposes a draft article for the WTO to regulate these mandates in Section III.

I. Should Local Storage Requirements be Regulated Directly Under the WTO Law?

As Chapter Three has previously introduced, the WTO recognizes the urgent need to address e-commerce issues within the framework of international trade, leading to the inception of the JSI. Despite these efforts, the pre-internet GATS may gradually become outdated in handling the concerns arising from the local storage requirements, as evidenced by the emergence of the LCF provisions.

The adverse economic impact resulting from local storage requirements cannot be overlooked. The findings of the OECD-WTO Business Survey in 2022 shed light on businesses' concerns over the negative impact of local storage requirements.[528] With over

[527] Japan JSI Proposal, ¶ 3.8; US JSI Proposal, ¶ 2.
[528] CHIARA DEL GIOVANE ET AL., *supra* note 14, at 20.

doi:10.6342/NTU202402499

400 views and 85 comprehensive responses obtained from 32 countries, this survey, designed to explore the nuances of data policies affecting data movement and storage, reveals that businesses perceive an increase in data management costs associated with local data storage measures.[529]

Notably, a significant proportion of respondents expressed concerns that more stringent data localization measures could impede their ability to operate internationally.[530] Moreover, the survey indicates widespread uncertainty among businesses regarding the efficacy of data localization measures in achieving broader public policy objectives such as domestic innovation, privacy protection, and data security.[531] Therefore, this thesis suggests that local storage requirements should be regulated directly under the WTO for the following reasons.

First, local storage requirements may result in unnecessary economic inefficiency. For instance, researchers suggested that the PDPL is anticipated to have an adverse effect on the Russian economy, resulting in a 0.27% decrease in GDP (approximately 286 billion rubles) due to companies choosing to exit or avoid entering the Russian market rather than adhering to the data localisation mandate.[532] In addition, governments advocate for the prohibition of data localisation measures in international trade relations mainly based on economic rationales.[533]

[529] CHIARA DEL GIOVANE ET AL., *supra* note 14, at 20.
[530] *Id.*
[531] *Id.*
[532] Helena Ursic ET AL., *supra* note 40, at 18.
[533] *See e.g.* Japan JSI proposal; US JSI proposal; *TPP Chapter Summary of Electronic Commerce*, UNITED STATES TRADE REPRESENTATIVE, https://ustr.gov/sites/default/files/TPP-ChapterSummary-Electronic-Commerce.pdf (last visited Apr. 11, 2024); *TPP Outcomes: Trade in the Digital Age*, AUSTL. GOV. DEPT. FOREIGN AFF. & TRADE, https://www.dfat.gov.au/trade/agreements/not-yet-in-force/tpp/Pages/outcomes-trade-in-the-digital-age (last visited Apr. 11, 2024).

doi:10.6342/NTU202402499

Second, the GATS is inadequate in addressing the negative trade impact of local storage requirements. These requirements inevitably impose compliance costs on enterprises lacking computing facilities within the markets they serve. However, as discussed in Chapter Three, this impact does not necessarily constitute a violation of GATS Article XVI(2)(a), (c), or XVII:1. Furthermore, GATS Articles XVI and XVII do not apply to certain modes of supply in specific service sectors where no specific commitments exist. Therefore, the GATS cannot effectively mitigate the compliance costs imposed on services and service suppliers.

Third, there are potentially less-trade restrictive alternatives to achieving certain local storage mandates. For instance, requirements mandating data encryption, database security with appropriate authentication measures, and adequate access control mechanisms can also achieve the objective of data protection.[534] Consequently, some Members might impose local storage requirements for reasons of economic protectionism rather than legitimate national objectives.

Fourth, local storage requirement measures raise cybersecurity risks by hindering the mobility of threat data essential for detecting and addressing cyber threats globally.[535] This results in the proliferation of additional databases within countries, which may expose data to heightened vulnerabilities, potentially facilitating unauthorized access by hackers and raising significant security concerns.[536]

Fifth, the WTO potentially offers remedies for mitigating the economic inefficiencies arising from local storage requirements as a rule-based multilateral organization. Bagwell and Staiger assert that the WTO's structure as a rule-based multilateral platform, along

[534] *See generally* Omotunde & Ahmed, *supra* note 332.
[535] CHIARA DEL GIOVANE ET AL., *supra* note 14, at 23.
[536] Helena Ursic ET AL., *supra* note 40, at 11.

doi:10.6342/NTU202402499

with its core principles of reciprocity and non-discrimination, illustrates Members' aim to remove the inefficiencies resulting from their unilateral trade policies.[537]

This thesis acknowledges that the economic rationale underpinning the WTO's establishment and its core principles may not align with regulating local storage requirements within the multilateral legal framework. Moreover, it does not argue that the economic inefficiency resulting from unilateral trade policies equates to that of such requirements. Instead, this thesis merely underscores the advantage of the WTO as a rule-based multilateral institution capable of offering consistent solutions to address the economic inefficiencies resulting from such measures.

The trade impact of local storage requirement measures cannot be understated, as these requirements have the potential to disrupt global supply chains and impede market access for cross-border service suppliers. Hence, this thesis suggests that such requirements should be regulated directly under WTO law. By establishing a uniform multilateral framework to restrict local storage requirements, the WTO can mitigate the fragmentation of such requirements worldwide, reduce compliance costs for enterprises, and uphold the principles of free and fair trade.

II. Local Storage Requirements Should be Explicitly Restricted Within the Framework of E-Commerce.

While revising existing GATS to include provisions regulating local storage requirements remains a potential approach, it may not fully address the evolving trade implications of such requirements, which extend beyond their impact on services over time. Recognizing the multifaceted adverse effects of local storage requirements,

[537] *See generally* Kyle Bagwell & Robert W. Staiger, an Economic Theory of GATT, 89(1) THE AM. ECON. REV. 215 (1999).

doi:10.6342/NTU202402499

particularly within the e-commerce domain, this thesis advocates for their prohibition within this context.

Countries advocate for the prohibition of data localisation measures primarily due to concerns regarding their adverse trade implications stemming from the financial burdens associated with potential investment costs in establishing or leasing data servers in markets where businesses aim to operate.[538] Recognizing the multifaceted nature of the trade impact of local storage requirements, particularly within the e-commerce context, this thesis suggests that restricting such requirements within the future WTO e-commerce agreement may represent the most efficient approach.

Restricting these requirements within a future WTO e-commerce agreement effectively mitigates the core trade impacts of mandates on using local computing facilities. This regulatory approach may comprehensively address their implications on services and other trade aspects within the WTO's regulatory framework.

Notably, local storage requirements encompass both digital data storage and physical document retention mandates. Nonetheless, However, the LCF provisions in RTAs and DEAs primarily focus on data localization measures related to digital data storage. Thus, it can be inferred that Members generally do not view the trade implications of physical document retention as part of the concerns related to data localization measures.

This thesis acknowledges that mandates on physical document retention may also have adverse trade impacts. However, given the concerns raised by Members regarding

[538] *See e.g.* Japan JSI proposal; US JSI proposal; *TPP Chapter Summary of Electronic Commerce*, UNITED STATES TRADE REPRESENTATIVE, https://ustr.gov/sites/default/files/TPP-ChapterSummary-Electronic-Commerce.pdf (last visited Apr. 11, 2024); *TPP Outcomes: Trade in the Digital Age*, AUSTL. GOV. DEPT. FOREIGN AFF. & TRADE, https://www.dfat.gov.au/trade/agreements/not-yet-in-force/tpp/Pages/outcomes-trade-in-the-digital-age (last visited Apr. 11, 2024).

doi:10.6342/NTU202402499

the prohibition of local storage requirements primarily focus on the trade impact of digital data storage, this thesis does not address whether mandates on physical document retention should or should not be restricted within the WTO. Instead, the discussion centers on how mandates requiring the local storage of digital data should be regulated under a future WTO e-commerce agreement in the following section.

III. The Proposed Draft Article.

Although draft texts addressing data localization are not present in the draft chair's text issued on June 28, 2024,[539] this thesis aims to propose a draft article regulating local storage requirements beyond the JSI agenda. This proposal could also serve as a potential reference under the World Trade Organization in the long-term discussion of a multilateral E-commerce agreement. Consequently, this draft article is not intended for the current JSI negotiating process but seeks to potentially address the WTO E-commerce agreement in the future.

This thesis proposes the following draft article to regulate local storage requirement measures within the context of E-commerce:

Article X General Prohibition on Local Data Storage Requirements (“Article X”)

1. Members recognise that each Member may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications.

[539] WTO Electronoic Commerce Negotiations, Draft Chair’s Text, WTO Doc INF/ECOM/86 (June 28, 2024).

doi:10.6342/NTU202402499

2. No Member shall require a covered person [540] to use or locate computing facilities[541] in that Member's territory as a condition for conducting business in that territory.
3. A Member may maintain a measure inconsistent with paragraph 2 provided that such a measure is listed in, and meets the conditions of, the Annex on Article X Exemptions.
4. Nothing in this Article shall prevent a Member from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) is necessary to achieve the objective.

A. Rationale of the Proposed Paragraph 1 of Article X.

The proposed paragraph 1 of Article X is identical to paragraph 1 of Article 14.13 of the CPTPP.[542] The rationale behind the proposed paragraph 1 of Article X lies in recognizing Members' regulatory autonomy and the need to respect their sovereignty in crafting policies related to local data storage requirements. While it is critical to prevent such requirements from becoming trade barriers, it is equally important to acknowledge the rights of WTO Members to regulate and introduce new regulations within their territories.

The GATS of the WTO also uphold this principle in its preamble,[543] affirming the sovereignty of Members to enact measures that serve their national policy objectives.

[540] The definition of a "covered person" is proposed as follows: 1. "covered person" means: (i) covered enterprise; or (ii) a natural person of the other Member; 2. "covered enterprise" means an enterprise of a Member that is owned or controlled, directly or indirectly, by a person of either Member.
[541]The definition of the term "computing facilities" is proposed as follows: computer servers and storage devices for processing or storing information for commercial use.
[542] CPTPP, art. 14.13(1).
[543] GATS, preamble, ("Recognizing the right of Members to regulate, and to introduce new regulations, on

doi:10.6342/NTU202402499

Furthermore, an analysis of existing provisions, as previously discussed in Chapter Four, section IV, reveals that most LCF provisions within RTAs recognize and respect the regulatory autonomy of each party regarding the location of computing facilities.[544] Therefore, paragraph 1 of Article X is crafted to align with the data sovereignty and demonstrate respect for Members' regulatory autonomy concerning their local data storage requirement measures.

B. Rationale of the Proposed paragraph 2 of Article X.

The proposed paragraph 2 of Article X refers to paragraph 2 of Article 14.13 of the CPTPP, a regulatory approach that is widespread across numerous RTAs encompassing the LCF provisions.[545] This thesis agrees with the rationale of Article 14.13(2) which aims to prevent local storage requirements from incurring "expensive and unnecessarily redundant data centres in every market they seek to serve",[546] ensuring "countries cannot force businesses to build data storage centres or use local computing facilities."[547]

Firstly, requiring any covered person to use or locate computing facilities[548] as a condition for conducting business in any Member's territory becomes a fundamental trade

---

the supply of services within their territories in order to meet national policy objectives and, given asymmetries existing with respect to the degree of development of services regulations in different countries, the particular need of developing countries to exercise this right;").

[544] *See e.g.*, TPP, art. 14.13(1); SAFTA, art. 24(1); Singapore–Sri Lanka FTA, art. 9.10(1); Australia–Peru FTA, art. 13.12(1); CPTPP, art. 14.13(1); ASEAN E-commerce Agreement, art. 7(6)(a); Australia–Indonesia CEPA, art. 13.12(1); Australia–Hong Kong FTA, art. 11.8(1); ASDEA, art. 24(1); RCEP, art. 12.14(1); Australia–UK FTA, art. 14.11(1); Singapore–UK DEA, art. 8.61-G(1); New Zealand–UK FTA, art. 15.15(1); UK–Ukraine Digital Trade Agreement, art. 132-L(1).

[545] *See e.g.*, TPP, art. 14.13(2); SAFTA, art. 24(2), Singapore–Sri Lanka FTA, art. 9.10(2); Australia–Peru FTA, art. 13.12(2); CPTPP, art. 14.13(2); ASEAN E-commerce Agreement, art. 7(6)(a); Australia–Indonesia CEPA, art. 13.12(2); Australia–Hong Kong FTA, art. 11.8(1); ASDEA, art. 24(2); RCEP, art. 12.14(2); Australia–UK FTA, art. 14.11(2), Singapore–UK DEA, art. 8.61-G(2); New Zealand–UK FTA art. 15.15(2); UK–Ukraine Digital Trade Agreement, art. 132-L(2).

[546] *TPP Chapter Summary of Electronic Commerce*, UNITED STATES TRADE REPRESENTATIVE, https://ustr.gov/sites/default/files/TPP-ChapterSummary-Electronic-Commerce.pdf (last visited Apr. 11, 2024).

[547] *See Trans-Pacific Partnership (TPP) Outcomes and Background*, AUSTL. GOV. DEP'T FOREIGN AFF. AND TRADE, https://www.dfat.gov.au/trade/agreements/not-yet-in-force/tpp/Pages/outcomes-trade-in-the-digital-age (last visited Mar. 19, 2024).

[548] The definition of the term "computing facilities" is proposed as follows:

doi:10.6342/NTU202402499

barrier to cross-border trade in services and goods, particularly those reliant on internet platforms, to minimize operational costs and facilitate business expansion. Such requirements inherently contradict the advancement of the digital economy, which is poised to make substantial contributions to global GDP growth in the forthcoming decades.[549]

Secondly, as previously discussed, local storage requirements that request the use of local computing facilities, such as the measure at issue, can possibly offer hackers an additional point of entry and raise various security concerns instead of ensuring data security.[550] Moreover, there exist less trade-restrictive alternatives to fulfill the objectives of such requirements.

Thirdly, countries imposing local storage requirements mandating the use of local computing facilities may potentially lead to self-sanctions on their economies. For instance, researchers from ECIPE anticipate that Russian Federal Law No. 242-FZ lead to an overall adverse impact on the Russian economy in the long run, estimating a reduction of 0.27 percent in Russian GDP, primarily due to companies choosing to either exit or refrain from entering the Russian market rather than complying with the measure at issue,[551] even if such measure boosts local data centres' profits in the short term.[552]

In general, the proposed paragraph 2 aligns with broader normative principles of the WTO aimed at promoting non-discrimination in trade relations. By prohibiting the mandating use of domestic computer servers and storage devices as a condition for

computer servers and storage devices for processing or storing information for commercial use.
[549] Arya Devi, *DCO 2030: Digital Economy to Contribute 30% of Global GDP and Create 30 Million Jobs by 2030*, EDGE (Feb. 5, 2023), https://www.edgemiddleeast.com/business/dco-2030-digital-economy-to-contribute-30-of-global-gdp-and-create-30-million-jobs-by-2030.
[550] Helena Ursic ET AL., *supra* note 40, at 11.
[551] *Id.* at 18.
[552] *Id.*

doi:10.6342/NTU202402499

conducting business in any territory of a Member, the proposed paragraph 2 inherently upholds the principles of market access and national treatment. This principle can ensure that foreign entities are not unfairly disadvantaged by local data storage requirements when accessing the domestic markets of any Member.

Although some WTO Members remain opposed to the idea of restricting local storage requirements, the legal complexities surrounding these mandates have imposed significant compliance burdens on SMEs. Therefore, this thesis suggests a principle of prohibition on these mandates, while allowing regulatory discretion for Members through exemption lists.

C. Rationale of the Proposed Paragraph 3 of Article X.

As noted above in Chapter Four, Section IV, subsection C, the LCF provisions generally do not apply to government procurements and measures related to information held or processed by or on behalf of a party. In addition, sectors associated with sensitive data or data concerning national security, such as financial sectors and telecommunication sectors, may also be exempted from the scope of the LCF provisions.

This thesis recognizes that countries' national objectives should also be respected. For instance, accessibility to data is one legitimate concern for implementing local storage requirements, given the difficulties of accessing data from foreign jurisdictions. Therefore, it is fair to allow countries to impose local storage requirements ensuring their accessibility to data gathered by certain highly regulated service sectors, such as financial or telecommunication sectors.

Accordingly, the proposed paragraph 3 borrows the regulatory approach of GATS Article II:2, allowing Members to exempt certain service sectors from the application of

doi:10.6342/NTU202402499

the proposed paragraph 2. The design of each Member's exemption list can also draw inspiration from the format of the GATS List of Article II (MFN) Exemptions[553], which encompasses the following details: (i) sector or subsectors, (ii) description of measure indicating its inconsistency with Article X, (iii) intended duration, and (iv) conditions creating the need for the exemption.

By explicitly enumerating the service sectors that are exempted and the conditions necessitating such exemptions, exemption lists can enhance transparency regarding Members' decisions on local storage and processing requirements. This transparency clarifies the rationale behind exemptions and ensures Members are aware of the conditions under which such requirements apply. Moreover, explicit and comprehensive exemption lists contribute to better understanding and adherence to regulatory measures, thereby easing the challenges associated with regulatory compliance for businesses.

This clarity ensures that businesses are informed about the specific sectors exempt from certain local storage or processing requirements and provides a clearer understanding of the global landscape of these requirements. Consequently, this advances their strategic business operations in the e-commerce domain.

D. Rationale of the Proposed Paragraph 4 of Article X.

As noted above in Chapter Four, Section IV, subsection C, the major LCF provisions embody their own exception paragraphs, typically encompassing a GATS Article XIV-like language with looser criteria, providing an open-ended list of policy objectives to justify measures inconsistent therewith. WTO Members' support for an open-ended lists

[553] *See e.g.*, US List of Article II (MFN) Exemptions, WTO Doc GATS/EL/90/Suppl.3, Feb. 26, 1998, https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S006.aspx?Query=(@Symbol=%20gats/el/*)%20and%20((%20@Title=%20united%20states%20)%20or%20(@CountryConcerned=%20united%20states))&Language=ENGLISH&Context=FomerScriptedSearch&languageUIChanged=true#.

doi:10.6342/NTU202402499

of exception clause is also evidenced by the updated consolidated negotiating text,[554] which adopts the regulatory model of TPP Article 14.13(3) as specific exceptions to the prohibition on data localization measures:[555]

This thesis acknowledges that data sovereignty mandate is increasingly becoming the primary rationales for most countries to implement exclusive local storage requirements. However, it remains uncertain whether data sovereignty mandates can be encompassed within the existing subparagraphs of GATS Article XIV. Additionally, given the evolving nature of technology, the national objectives for imposing local storage requirements may expand as technology advances over time.

Hence, this thesis borrows the language from Article 14.13(3) of the CPTPP to propose an exception paragraph of Article X, allowing Members to justify their measures inconsistent with the proposed paragraph 2 when such measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and is necessary to achieve the objective. Under this specific exception clause, mandates such as data sovereignty are more likely to justify Members' exclusive local storage requirements than when invoked under the regulatory model of GATS Article XIV.

Overall, the decisive factor in ascertaining the justification for a local storage requirement under the proposed paragraph 4 will be the necessity test. This is because the majority of local storage requirements are typically implemented in a non-discriminatory manner, which generally does not constitute arbitrary or unjustifiable discrimination.

E. Applicable Security Exceptions in the E-Commerce Agreement

[554] WTO Electronoic Commerce Negotiations, Updated Consolidated Negotiation Text-November 2023, WTO Doc INF/ECOM/62/Rev.5 (Nov. 15, 2023).
[555] *Id.* at 32.

doi:10.6342/NTU202402499

This thesis proposes not to adopt a specific security exception clause under this draft article but rather to design a general security exception clause applicable to the entire e-commerce agreement.

While the design of such security exceptions is not addressed here, the contentious nature of security exceptions often prompts debates regarding their "self-judging" nature. Accordingly, the design of the security exception clause in the e-commerce agreement should clarify several key aspects as follows:

(i) Whether the invocation of the security exception clause can be subject to review by WTO adjudicative bodies;

(ii) To what extent the invocation can be "self-judging"

(iii) Whether Members invoking the security exception clause should still adhere to the principle of good faith and proportionality in their actions.

Since countries frequently justify local storage requirements on national security grounds, these clarifications are crucial for ensuring transparency and preventing the abuses of national security reasons from becoming a disguise of economic protectionism.

F. This Draft Article and Other Covered Agreements.

This draft article is not intended to be *lex specialis* to GATS and other WTO's covered agreements. Therefore, even if a local storage requirement is consistent with this draft article, it must still comply with obligations under GATS and other covered agreements.

In summary, this draft article aims to mitigate the trade impacts arising from local storage requirements within the e-commerce context, but it does not exempt them from obligations under other WTO's covered agreements.

doi:10.6342/NTU202402499

doi:10.6342/NTU202402499

CHAPTER SIX

CONCLUSION

Since the inception of the Internet in 1983, data has become a cornerstone of the digital economy. Data is critical for modern trade and production. However, governments are increasingly implementing data localisation policies to regulate where data can be processed and stored. These measures often lead to reduced trade output, productivity, and increased prices.

This thesis focuses on examining the trade impacts resulting from local storage requirements on services and analyzing how the WTO should regulate these mandates in the future. Local storage requirements mandate data controllers to store data within specific geographic regions. They impose constraints on strategic decisions regarding the location of computing facilities. This characteristic leads to compliance costs for establishing or leasing local data centers or servers, particularly affecting service suppliers lacking local storage facilities.

While GATS does not explicitly prohibit local storage requirements, some scholars assert that such requirements are inconsistent with GATS Article XVI:2(a), (c), as cross-border services do not necessitate a physical presence within the service delivery territory. However, whether the use of local data servers constitutes a physical or commercial presence is debatable.

Another relevant provision to regulate local storage requirements is GATS Article XVII:1. Nonetheless, local storage requirements only favour domestic services or service suppliers over foreign like competitors when domestic services suppliers possess local computing facilities while their counterparts do not. Therefore, whether these requirements violate GATS Article XVII:1 still depends on case-by-case analysis.

doi:10.6342/NTU202402499

Notably, GATS Articles XVI and XVII are binding only when Members commit to specific service sectors' modes of supply. Therefore, they may not adequately address the negative trade impacts of local storage requirements across any supply modes in all service sectors.

Due to the inefficiency of pre-internet covered agreements to handle e-commerce issues, the WTO incorporated e-commerce into its agenda with the 1998 Declaration on Global Electronic Commerce. The work programme on e-commerce eventually led to the formation of the plurilateral platform JSI.

In JSI discussions, some Members propose prohibiting data localization. The JSI discussions highlight that the pre-internet GATS and other covered agreements seem not to fully address the adverse impact of the emerging numbers of local storage requirements, evidenced by the proliferation of the LCF provisions across RTAs and DEAs since 2014.

The LCF provisions across RTAs and DEAs underline the need to address the negative trade impacts of local storage and processing requirements in this digital era. Such provisions typically reflect the stance of the US data localisation policy, emphasizing the prohibition of requirements mandating the use or location of computing facilities within a party's territory as conditions to conduct business. Despite similarities in prohibiting mandatory use or location of computing facilities, differences in scope and exceptions reflect the diverse interests and priorities of participating countries.

This thesis recognizes the importance of respecting the policy mandates driving local storage requirements pursued by WTO Members. However, it argues that such requirements should be directly restricted under the WTO to mitigate economic inefficiency resulting from every country's unilateral local storage requirement. Upon

doi:10.6342/NTU202402499

examining the practices and rationales for prohibiting such requirements in relation to trade, the thesis concludes that mandating physical document retention through local storage requirements is not a primary concern in the realm of data localization internationally.

Consequently, the thesis proposes a draft article that prohibits the requirements mandating the use or location of computing facilities as a condition for conducting business in any Member's territory. Nonetheless, this thesis also acknowledges that national objectives should be respected. For instance, ensuring accessibility to data is one legitimate concern behind local storage requirements, particularly due to challenges in accessing data from foreign jurisdictions. Consequently, it is reasonable for countries to impose local storage requirements for certain highly regulated service sectors, such as the financial and telecommunications sectors, to ensure they can access the necessary data. Accordingly, this thesis further proposes exemption lists that allow members to exempt certain service sectors from such obligations in the draft article.

In addition, given that national mandates for imposing local storage requirements may evolve as technology develops, this thesis proposes an exception paragraph for Article X. Inspired by Article 14.13(3) of the CPTPP, this exception provides an open-ended list of national objectives that Members can invoke for justification.

In terms of security exceptions, this thesis proposes having a general security exception clause for the entire e-commerce agreement instead of outlining a specific one for the draft article. The design of such security exceptions should clarify whether the invocation of the security exception clause can be reviewed by WTO adjudicative bodies, to what extent the invocation can be "self-judging," and whether Members invoking the clause should adhere to the principles of good faith and proportionality.

doi:10.6342/NTU202402499

To conclude, GATS appears inadequate in addressing the trade impact of local storage requirements from the perspectives of some WTO Members. Consequently, the thesis suggests explicit restrictions on local storage requirements under the WTO, particularly when they mandate the use of local computing facilities as prerequisites for conducting business in Members' territories. Drawing inspiration from the exceptions found in LCF provisions and GATS Article II:2, this thesis suggests the creation of exemption lists and more flexible exception criteria to strike a balance between policy objectives and trade facilitation. Notably, the proposed regulatory model merely seeks to mitigate the trade impacts of local storage requirements within the e-commerce context without exempting them from obligations under GATS or any other WTO's covered agreements.

doi:10.6342/NTU202402499

REFERENCES

Books

HART, CHRIS (2018), DOING A LITERATURE REVIEW: RELEASING THE RESEARCH IMAGINATION. 2nd ed.

NAEF, TOBIAS (eds.) (2023), DATA PROTECTION WITHOUT DATA PROTECTIONISM: THE RIGHT TO PROTECTION OF PERSONAL DATA AND DATA TRANSFERS IN EU LAW AND INTERNATIONAL TRADE LAW.

VAN DEN BOSSCHE, PETER & ZDOUC, WERNER (2017), THE LAW AND POLICY OF THE WORLD TRADE ORGANIZATION. 4th ed.

WEBER, ROLF H. & BURRI, MIRA (2012), CLASSIFICATION OF SERVICES IN THE DIGITAL ECONOMY.

Articles in Journals /Shorter Works in Collection

Aldaas, Abdullah (2021), *A Study on Electronic Payments and Economic Growth: Global Evidences,* 7 ACCOUNTING 409.

Alford, Roger P. (2011), *The Self-Judging WTO Security Exception*, 3 UTAH LAW REVIEW 697.

Leiner, Barry M. et al. (2009), *A Brief History of the Internet*., 39 ACM SIGCOMM COMPUTER COMMUNICATION REVIEW 22.

Bagwell, Kyle & Robert W. Staiger (1999), *an Economic Theory of GATT*, 89(1) THE AMERICAN ECONOMIC REVIEW 215.

Bayraktar, Murat & Neşe Algan (Selahattin Sarı et al. ed., 2019), *The Importance of SMEs on World Economies*, in INTERNATIONAL CONFERENCE ON EURASIAN ECONOMIES 2019, 56.

Fahey, Elaine (2023), *Does the EU's Digital Sovereignty Promote Localisation in Its Model Digital Trade Clauses*, 8(2) EUROPEAN PAPERS 503.

Ferracane, Martina (2018), *Data Flows & National Security: A Conceptual Framework to Assess Restrictions on Data Flows Under GATS Security Exception*, 21(1) DIGITAL POLICY REGULATION AND GOVERNANCE 44.

doi:10.6342/NTU202402499

Ganne, Emmanuelle & Kathryn Lundquist (2019), *The Digital Economy, GVCs and SMEs*, in GLOBAL VALUE CHAIN DEVELOPMENT REPORT 2019: TECHNOLOGICAL INNOVATION, SUPPLY CHAIN TRADE, AND WORKERS IN A GLOBALIZED WORLD 121.

Han, Sanghyun (2024), *Data and Statecraft: Why and How States Localize Data*, 26(2) BUSINESS AND POLITICS 263.

Hummel, Patrik, et alt. (2021), *Data Sovereignty: a Review*, 8(1) BIG DATA & SOCIETY 1.

Leiner, Barry M. et al. (2009), *A Brief History of the Internet*., 39 ACM SIGCOMM COMPUTER COMMUNICATION REVIEW 22.

Liu, Han-Wei (Pasha L. Hsieh & Bryan Mercurio eds., 2019), *Data Localization and Digital Trade Barriers: ASEAN in Megaregionalism*, in ASEAN LAW IN THE NEW REGIONAL ECONOMIC ORDER: GLOBAL TRENDS & SHIFTING PARADIGMS 371.

Marchetti, Juan A. & Petros C. Mavroidis (2011), *The Genesis of the GATS (General Agreement on Trade in Services),* 22(3) THE EUROPEAN JOURNAL OF INTERNATIONAL LAW 689.

Omotunde, Habeeb & Maryam Ahmed (2023), *A comprehensive review of security measures in database systems: Assessing authentication, access control, and beyond*, 2023 MESOPOTAMIAN JOURNAL OF CYBERSECURITY 115.

Peng, Shin-yi & Han-wei Liu (2017), *The Legality of Data Residency Requirements: How Can the Trans-Pacific Partnership Help*, 51(2) JOURNAL OF WORLD TRADE 183.

Peng, Shin-yi (2014), *Regulating New Services Through Litigation?–Electronic Commerce as a Case Study on the Evaluation of 'Judicial Activism' in the WTO*, 48(6) JOURNAL OF WORLD TRADE 1189.

Quan, Xiaolian (2020), *The Governance of Cross-Border Data Flows in Trade Agreements: Is the CPTPP Framework an Ideal Way out*, 15 FRONTIERS OF LAW IN CHINA 253.

Timmers, Paul (Hannes Werthner et al. ed., 2023), *Sovereignty in the Digital Age*, *in* INTRODUCTION TO DIGITAL HUMANISM 571.

Todd Allee & Andrew Lugg (2016), *Who Wrote the Rules for the Trans-Pacific Partnership,* 3 RESEARCH & POLITICS 1.

Ursic, Helena et al. (2017), *Data Localisation Measures and Their Impacts on Data Science*, in RESEARCH HANDBOOK IN DATA SCIENCE AND LAW 322.

doi:10.6342/NTU202402499

Wunsch-Vincent, Sacha (2003), *The Digital Trade Agenda of the U.S.: Parallel Tracks of Bilateral, Regional and Multilateral Liberalization*, 58(1) AUSSENWIRTSCHAFT 7.

Nonperiodic Papers, Reports and Articles

BAUER, MATTHIAS ET ALT. (2014), THE COSTS OF DATA LOCALISATION: FRIENDLY FIRE ON ECONOMIC RECOVERY.

BAUER, MATTHIAS ET AL. (2016), UNLEASHING INTERNAL DATA FLOWS IN THE EU: AN ECONOMIC ASSESSMENT OF DATA LOCALISATION MEASURES IN THE EU.

CORY, NIGEL & DASCOLI, LUKE (2021), HOW BARRIERS TO CROSS-BORDER DATA FLOWS ARE SPREADING GLOBALLY, WHAT THEY COST, AND HOW TO ADDRESS THEM.

FEFER, RACHEL F. (2020), INTERNET REGIMES AND WTO E COMMERCE NEGOTIATIONS.

HILL, JONAH FORCE (2014), THE GROWTH OF DATA LOCALIZATION POST-SNOWDEN: ANALYSIS AND RECOMMENDATIONS FOR U.S. POLICYMAKERS AND BUSINESS LEADERS.

GIOVANE, CHIARA DEL ET AL. (2023), OECD TRADE POLICY PAPERS NO. 278 THE NATURE, EVOLUTION AND POTENTIAL IMPLICATIONS OF DATA LOCALISATION MEASURES.

ISMAIL, YASMIN (2020), E-COMMERCE IN THE WORLD TRADE ORGANIZATION: HISTORY AND LATEST DEVELOPMENTS IN THE NEGOTIATIONS UNDER THE JOINT STATEMENT.

KHASANOVA, LILIYA & TAI, KATHARIN (2023), AN AUTHORITARIAN APPROACH TO DIGITAL SOVEREIGNTY? RUSSIAN AND CHINESE DATA LOCALISATION MODELS.

LÓPEZ-GONZÁLEZ, JAVIER & JOUANJEAN, M. (2017), OECD TRADE POLICY PAPERS NO.205 DIGITAL TRADE: DEVELOPING A FRAMEWORK FOR ANALYSIS.

Treaties

WTO Covered Agreements

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

doi:10.6342/NTU202402499

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

WTO Agreement: Marrakesh Agreement Establishing the World Trade Organization, April 15, 1994, 1867 U.N.T.S. 154, 33 I.L.M. 1144 (1994).

RTAs

Agreement Between Japan and Mongolia for an Economic Partnership, Japan–Mongolia, February 10, 2015, https://rtais.wto.org/UI/PublicShowMemberRTAIDCard.aspx?rtaid=835.

Agreement Between the United States of America and Japan Concerning Digital Trade, Japan–US, October 7, 2019, https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf.

Agreement between the United States of America, the United Mexican States, and Canada, US–Mexico–Canada, November 30, 2018, https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between.

ASEAN Agreement on Electronic Commerce, January 22, 2019, https://agreement.asean.org/media/download/20190306035048.pdf.

Australia Hong Kong Free Trade Agreement and Associated Investment Agreement, Hong kong–Australia, March 26, 2019, https://www.dfat.gov.au/trade/agreements/in-force/a-hkfta/a-hkfta-text/Pages/default.

Australia–Singapore Digital Economy Agreement, Australia-Singapore, August 6, 2020, https://www.dfat.gov.au/trade/services-and-digital-trade/australia-and-singapore-digital-economy-agreement.

Australia–United Kingdom Free Trade Agreement, Australia-United Kingdom, December 17, 2021, https://www.dfat.gov.au/trade/agreements/in-force/aukfta/official-text.

Comprehensive and Progressive Agreement for Trans-Pacific Partnership, March 8, 2018, https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/cptpp/comprehensive-and-progressive-agreement-for-trans-pacific-partnership-text-and-resources/.

doi:10.6342/NTU202402499

Digital Economy Agreement between the United Kingdom of Great Britain and Northern Ireland and the Republic of Singapore, Singapore–UK, February 25, 2022, https://www.gov.uk/government/collections/uk-singapore-digital-economy-agreement.

Digital Economy Partnership Agreement, Chile–New Zealand–Singapore, June 12, 2020, https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement-depa/depa-text-and-resources/.

Digital Partnership Agreement between the Government of the Republic of Korea and the Government of the Republic of Singapore, Korea–Singapore, November 21, 2022, https://www.fta.go.kr/webmodule/_PSD_FTA/ksdpa/1/DPA_eng.pdf.

Digital Trade Agreement between the United Kingdom of Great Britain and Northern Ireland and Ukraine, UK–Ukraine, March 20, 2023, https://www.gov.uk/government/publications/ukukraine-digital-trade-agreement-cs-ukraine-no22023.

Free Trade Agreement Between the Democratic Socialist Republic of Sri Lanka and the Republic of Singapore, Singapore–Sri Lanka, January 23, 2018, https://edit.wti.org/document/show/290ae462-2914-4e19-b516-678bbcd4f8e1.

Free Trade Agreement between the EFTA States and the Republic of Moldova, June 27, 2023, https://edit.wti.org/document/show/5dd788d0-ccd2-4392-9744-58eb6a3876a4?page=2.

Free Trade Agreement between the European Union and New Zealand, EU–New Zealand, July 9, 2023, https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/new-zealand/eu-new-zealand-agreement/text-agreement_en.

Free Trade Agreement between the Republic of Chile and the Federative Republic of Brazil, Brazil–Chile, November 21, 2018, https://edit.wti.org/document/show/e62cfb4c-abbf-43d9-ae34-a15c7d057ab4.

Free Trade Agreement between the United Kingdom of Great Britain and Northern Ireland and New Zealand, New Zealand–UK, February 28, 2022, https://www.gov.uk/government/collections/free-trade-agreement-between-the-united-kingdom-of-great-britain-and-northern-ireland-and-new-zealand.

doi:10.6342/NTU202402499

Indonesia Australia Comprehensive Economic Partnership Agreement, Indonesia–Australia, March 4, 2019, https://www.dfat.gov.au/trade/agreements/in-force/iacepa/indonesia-australia-comprehensive-economic-partnership-agreement.

Peru Australia Free Trade Agreement, Peru–Australia, June 24, 2020, https://www.dfat.gov.au/trade/agreements/in-force/pafta/full-text/Pages/fta-text-and-associated-documents.

Regional Comprehensive Economic Partnership Agreement, December 15, 2020, https://www.dfat.gov.au/trade/agreements/in-force/rcep/rcep-text.

Singapore Australia Free Trade Agreement, Singapore–Australia, September 5, 2003, https://www.dfat.gov.au/trade/agreements/in-force/safta/official-documents.

Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the One Part, and the United Kingdom of Great Britain and Northern Ireland, of the Other Part, EU–UK, December 24, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22021A0430%2801%29.

Transpacific Partnership Agreement, February 4, 2016, https://ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-full-text.

Others

Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, December 13, 2007, 2007 O.J. (C306) 1.

Cases & Briefs

Appellate Body Reports

Appellate Body Report, *Argentina — Measures Relating to Trade in Goods and Services*, WTO Doc WT/DS453/AB/R (adopted on May 9, 2016).

Appellate Body Report, *Brazil — Measures Affecting Imports of Retreaded Tyres*, WTO Doc WT/DS332/AB/R (adopted on December 17, 2007).

Appellate Body Report, *Canada — Certain Measures Affecting the Automotive Industry*, WTO Doc WT/DS139/AB/R (adopted on June 19, 2000).

Appellate Body Report, *Colombia — Measures Relating to the Importation of Textiles, Apparel and Footwear*, WTO Doc WT/DS461/AB/R (adopted on June 22, 2016).

doi:10.6342/NTU202402499

Appellate Body Report, *European Communities — Measures Affecting Asbestos and Products Containing Asbestos*, WTO Doc WT/DS135/AB/R (adopted on April 5, 2001).

Appellate Body Report, *European Communities — Regime for the Importation, Sale and Distribution of Bananas*, WTO Doc WT/DS27/AB/R (adopted on September 25, 1997).

Appellate Body Report, *European Communities — Measures Prohibiting the Importation and Marketing of Seal Products*, WTO Doc WT/DS401/AB/R (adopted on June 18, 1997).

Appellate Body Report, *European Communities — Conditions for the Granting of Tariff Preferences to Developing Countries*, WTO Doc WT/DS246/AB/R (adopted on April 20, 2004).

Appellate Body Report, *India — Certain Measures Relating to Solar Cells and Solar Modules*, WTO Doc WT/DS456/AB/R (adopted on October 14, 2016).

Appellate Body Report, *Korea — Measures Affecting Imports of Fresh, Chilled and Frozen Beef*, WTO Doc WT/DS161/AB/R (adopted on January 10, 2001).

Appellate Body Report, *Mexico — Tax Measures on Soft Drinks and Other Beverages*, WTO Doc WT/DS308/AB/R (adopted on March 24, 2006).

Appellate Body Report, *United States — Tax Treatment for "Foreign Sales Corporations"*, WTO Doc WT/DS108/AB/RW (adopted on January 29, 2002).

Appellate Body Report, *United States — Standards for Reformulated and Conventional Gasoline*, WTO Doc WT/DS2/AB/R (adopted on May 20, 1996).

Appellate Body Report, *United States — Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WTO Doc WT/DS285/AB/R (adopted on April 20, 2005).

Appellate Body Report, *United States — Sunset Reviews of Anti-Dumping Measures on Oil Country Tubular Goods from Argentina*, WTO Doc WT/DS268/AB/R (adopted on December 17, 2004).

Appellate Body Report, *United States — Import Prohibition of Certain Shrimp and Shrimp Products*, WTO Doc WT/DS58/AB/R (adopted on November 6, 1998).

Panel Reports

doi:10.6342/NTU202402499

Panel Report, *Argentina — Measures Relating to Trade in Goods and Services*, WTO Doc WT/DS453/R (adopted on May 9, 2016).

Panel Report, *China — Certain Measures Affecting Electronic Payment Services*, WTO Doc WT/DS413/R (adopted on August 31, 2012).

Panel Report, *Colombia — Argentina — Measures Affecting the Export of Bovine Hides and the Import of Finished Leather*, WTO Doc WT/DS155/R (adopted on February 16, 2001).

Panel Report, *Colombia — Measures Relating to the Importation of Textiles, Apparel and Footwear*, WTO Doc WT/DS461/R (adopted on June 22, 2016).

Panel Report, *Dominican Republic — Measures Affecting the Importation and Internal Sale of Cigarettes*, WTO Doc WT/DS302/R (adopted on May 19, 2005).

Panel Report, *European Communities — Measures Affecting Asbestos and Products Containing Asbestos*, WTO Doc WT/DS135/R (adopted on April 5, 2001).

Panel Report, *European Communities — Regime for the Importation, Sale and Distribution of Bananas*, WTO Doc WT/DS27/R (adopted on May 22, 1997).

Panel Report, *European Communities — Selected Customs Matters* WTO Doc WT/DS315/R, (adopted on December 11, 2006).

Panel Report, *Korea — Measures Affecting Imports of Fresh, Chilled and Frozen Beef*, WTO Doc WT/DS161/R (adopted on January 10, 2001).

Panel Report, *Thailand — Customs and Fiscal Measures on Cigarettes from the Philippines*, WTO Doc WT/DS371/R (adopted on July 15, 2011).

Panel Report, *United States — Certain Country of Origin Labelling (COOL) Requirements*, WTO Doc WT/DS384/R (adopted on July 23, 2012).

Panel Report, *United States — Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WTO Doc WT/DS285/R (adopted on April 20, 2005).

Panel Report, *Colombia —United States — Anti-Dumping Measures on Certain Hot-Rolled Steel Products from Japan*, WTO Doc WT/DS184/R (adopted on August 23, 2001).

Panel Report, *United States — Origin Marking Requirement,* WTO Doc WT/DS597/R (under appeal on January 26, 2023).

doi:10.6342/NTU202402499

GATT Reports

GATT Panel Report, *EEC — Regulation on Imports of Parts and Components*, WTO Doc L/6657 (adopted on May 16, 1990) 37S/132.

GATT Panel Report, *Italy — Discrimination Against Imported Agricultural Machinery*, WTO Doc L/833 (adopted on October 23, 1958) SR.13/8.

GATT Panel Report, *United States — Trade Measures Affecting Nicaragua*, WTO Doc L/6053.

GATT Panel Report, *United States — Section 337 of the Tariff Act of 1930*, WTO Doc L/6439 (adopted on November 7, 1989) 36S/345.

Other Cases

Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016).

United States v. Microsoft Corp., 584 U.S. ___, 138 S. Ct. 1186 (2018).

Joined Cases C-293/12 & C-594/12, Digital Rights Ireland Ltd v Minister for Commc'n, Marine and Natural Resources, ECLI:EU:C:2014:238 (June 10, 2014)

Other International Documents

WTO Documents

Committee on Trade and Development, Interim review of progress in the implementation of the Work Programme on Electronic Commerce - Communication from the Chairman of the Committee on Trade and Development, WTO Doc WT/GC/23, April 7, 1999.

Council for Trade in Goods, Interim review of progress in the implementation of the Work Programme on Electronic Commerce - Communication from the Chairman of the Council for Trade in Goods, WTO Doc WT/GC/24, April 9, 1999).

Council on Trade in Services, Guidelines for the Scheduling of Specific Commitments und the General Agreement on Trade in Services (GATS), WTO Doc S/L/92, March 28, 2001.

doi:10.6342/NTU202402499

Council for Trade in Services, Work Programme on Electronic Commerce - interim report to the General Council, WTO Doc S/C/8, March 31, 1999.

Council for Trade in Services, Work Programme on Electronic Commerce - Report by the Chairman of the Council for Trade in Services to the General Council, WTO Doc S/C/43, June 30, 2014.

Council for Trade in Services, Work Programme on Electronic Commerce – Communication by the United States, WTO Doc S/C/W/359, December 17, 2014.

Council for Trade in Services, Work Programme on Electronic Commerce – Report by the Chairman of the Council for Trade in Services to the General Council, WTO Doc S/C/47, July 17, 2015.

Council for Trade-Related Aspects of Intellectual Property Rights, Interim review of progress in the implementation of the Work Programme on Electronic Commerce – Communication from the Chairman of the Council for TRIPS, WTO Doc WT/GC/21, March 23, 1999.

General Council, Work Programme on Electronic Commerce - Report of panel discussion on “digital industrial policy and development” - Communication from the African Group, WTO Doc JOB/GC/133, July 21, 2017.

General Council, Work Programme on Electronic Commerce, Non-paper from the United States, WTO Doc JOB/GC/94, July 4, 2016.

General Council, Council for Trade in Goods, Council for Trade in Services, Council for Trade-Related Aspects of Intellectual Property Rights, Committee on Trade and Development, Work Programme on Electronic Commerce, Trade Policy, the WTO, and the Digital Economy, Communication from Canada, Chile, Colombia, Côte d'Ivoire, the EU, the Republic of Korea, Mexico, Montenegro, Paraguay, Singapore and Turkey, WTO Doc JOB/GC/116, JOB/CTG/4 JOB/SERV/248, JOB/IP/21 JOB/DEV/42, January 13, 2017.

Joint Statement on Electronic Commerce, WTO Doc WT/L/1056, January 25, 2019.

Joint Statement on Electronic Commerce Initiative: Communication from China, WTO Doc INF/ECOM/19, April 24, 2019.

Joint Statement on Electronic Commerce Initiative: Communication from European Union, WTO Doc INF/ECOM/22, April 26, 2019.

doi:10.6342/NTU202402499

Joint Statement on Electronic Commerce Initiative Proposal for the Exploratory Work by Japan, WTO Doc JOB/GC/177, April 12, 2018.

Joint Statement on Electronic Commerce Initiative: Communication from the United States, WTO Doc INF/ECOM/5, March 25, 2019.

Ministerial Conference, Joint Statement on Electronic Commerce, WTO Doc WT/MIN(17)/60, December 13, 2017.

Ministerial Conference, Nairobi Ministerial Decision, WTO Doc WT/MIN(15)/DEC, December 21, 2015.

Ministerial Conference, Ministerial Declaration of 14 November 2001, WTO Doc WT/MIN(01)/DEC/1, November 20, 2001.

Ministerial Conference, Ministerial Declaration of 20 May 1998 on Global Electronic Commerce, WTO Doc WT/MIN(98)/DEC/2, May 25, 1998.

Russian Federation Schedule of Specific Commitments, Trade in Services, WTO Doc GATS/SC/149, November 5, 2012.

US List of Article II (MFN) Exemptions, WTO Doc GATS/EL/90/Suppl.3, February 26, 1998.

WTO Electronoic Commerce Negotiations, Updated Consolidated Negotiation Text-November 2023, WTO Doc INF/ECOM/62/Rev.5, November 15, 2023.

WTO Electronoic Commerce Negotiations, Draft Chair's Text, WTO Doc INF/ECOM/86, June 28, 2024.

EU Documents

Council Directive 95/46, 1995 (EC).

Council Directive 2006/24/EC, 2002/58/EC, [2006] O.J. L 105/54.

Council Conclusions, Oct. 1-2, 2020, EUCO 13/20 (2020).

National Statutes, laws or regulations

Constitution of the Russian Federation, December 12, 1993.

Companies (Accounts) Rules 2014, 2014, Rule 3(5) (India).

doi:10.6342/NTU202402499

My Health Records Act 2012 (Austl.).

Russian Federation Federal Law on Personal Data, 2014 (No. 242-FZ).

Unpublished Manscripts, Internet and Other Sources

Smale, Alison (February 16, 2014), *Merkel Backs Plan to Keep European Data in Europe*, THE N.Y. TIMES, http://www.nytimes.com/2014/02/17/world/europe/merkel-backs-plan-to-keep-europeandata-in-europe.html?hp&_r=0.

Association of Southeast Asian Nations, The Regional Comprehensive Economic Partnership (RCEP), https://asean.org/our-communities/economic-community/integration-with-global-economy/the-regional-comprehensive-economic-partnership-rcep/.

Australia Government Department of Foreign Affairs & Trade, *TPP Outcomes: Trade in the Digital Age*, https://www.dfat.gov.au/trade/agreements/not-yet-in-force/tpp/Pages/outcomes-trade-in-the-digital-age.

4. Applications to the CPTPP: the United Kingdom, China, Taiwan and South Korea, PARLIAMENT OF AUSTRALIA, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Foreign_Affairs_Defence_and_Trade/CPTPPMembership/Report/section?id=committees%2Freportjnt%2F024826%2F78218.

Brad Carr et al. (December 22, 2020), *Data Localization: Costs, Tradeoffs, and Impacts Across the Economy*, Institute of International Finance,https://www.iif.com/portals/0/Files/content/Innovation/12_22_2020_data_localization.pdf.

Cate, Fred H. (2008), *Provincial Canadian Geographic Restrictions on Personal Data in the Public*, HUNTON ANDREWS KURTH LLP, https://www.huntonak.com/files/Publication/2a6f5831-07b6-4300-af8d-ae30386993c1/Presentation/PublicationAttachment/0480e5b9-9309-4049-9f25-4742cc9f6dce/cate_patriotact_white_paper.pdf.

Castro, Daniel & Travis Korte (November 3, 2013), *Data Innovation 101*, CENTER FOR DATA INNOVATION, https://www.datainnovation.org/2013/11/data-innovation-101/.

China to speed up accession to CPTPP, CHINA INTERNATIONAL IMPORT EXPO (March 22, 2024),

doi:10.6342/NTU202402499

https://english.www.gov.cn/news/202403/22/content_WS65fcddf2c6d0868f4e8e555c.html.

COMMITTEE OF EXPERTS UNDER THE CHAIRMANSHIP OF JUSTICE B.N. SRIKRISHNA (July 27, 2018), A FREE AND FAIR DIGITAL ECONOMY PROTECTING PRIVACY, EMPOWERING INDIANS, https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.

Cory, Nigel (March 8, 2019), *Comments on India's Draft National E-Commerce Policy*, INFORMATION TECHNOLOGY & INNOVATION FOUNDATION, https://itif.org/publications/2019/03/08/comments-indias-draft-national-e-commerce-policy.

CPTPP: Overview and Issues for Congress, CONGRESSIONAL RESEARCH SERVICE (June 16, 2023), https://crsreports.congress.gov/product/pdf/IF/IF12078.

Craymer, Lucy & Joe Cash (August 1, 2023), *Biggest Hurdles to China Entry into Trans-Pacific Trade Pact are Political*, REUTERS, https://www.reuters.com/world/biggest-hurdles-china-entry-into-trans-pacific-trade-pact-are-political-2023-07-31/.

Crosby, Daniel (2016), *Analysis of Data Localization Measures Under WTO Services Trade Rules and Commitments*, INTERNATIONAL CENTER FOR TRADE AND SUSTAINABLE DEVELOPMENT & WORLD ECONOMIC FORUM E15INITIATIVE, http://e15initiative.org/wpcontent/uploads/2015/09/E15-Policy-Brief-Crosby-Final.pdf,

Dash, Angelina (September 14, 2023), *Big Tech vs News Publishers: A Rights-Based Perspective*, CTR. FOR COMMC'N GOVERNANCE BLOG, https://ccgnludelhi.wordpress.com/category/internet-governance/.

Devi, Arya (February 5, 2023), *DCO 2030: Digital Economy to Contribute 30% of Global GDP and Create 30 Million Jobs by 2030*, EDGE, https://www.edgemiddleeast.com/business/dco-2030-digital-economy-to-contribute-30-of-global-gdp-and-create-30-million-jobs-by-2030.

Decree 53/2022 - Further Guidance on Data Localisation in Vietnam, VIETNAM BUS. L., https://vietnam-business-law.info/blog/2022/9/4/decree-532022-further-guidance-on-data-localisation-in-vietnam.

ELECTRONIC COMMERCE, https://www.wto.org/english/thewto_e/minist_e/mc11_e/briefing_notes_e/bfecom_e.htm.

doi:10.6342/NTU202402499

Elterman, Maria (January 23, 2017), *Why LinkedIn was banned in Russia,* IAPP, https://iapp.org/news/a/why-linkedin-was-banned-in-russia/.

Garcia-Israel, Katya & Julien Grollier (October 10, 2019), *Electronic Commerce Joint Statement: Issues in the Discussion Phase*, CUTS INTERNATIONAL GENEVA, https://www.cuts-geneva.org/?s=Electronic+Commerce+Joint+Statement%3A+Issues+in+the+Discussion+Phase.

Growth of digital economy outperforms overall growth across OECD (May 14, 2024), OECD, https://www.oecd.org/newsroom/growth-of-digital-economy-outperforms-overall-growth-across-oecd.htm.

Horizontal provisions for cross-border data flows and for personal data protection (May 18, 2018), EUROPEAN COMMISSION NEWSROOM, https://ec.europa.eu/newsroom/just/items/627665.

Howard, Rebecca (February. 4, 2016), *Trans-Pacific Partnership Trade Deal Signed, but Years of Negotiations Still to Come,* REUTERS, http://perma.cc/5DDA-2Z5B.

Ismail, Yasmin & Rashmi Jose (January 11, 2024), *E-Commerce Takes Centre Stage at World Trade Organization in Run-up to MC13*, INTERNATIONAL INSTITUTION FOR SUSTAINABLE DEVELOPMENT, https://www.iisd.org/Art.s/policy-analysis/e-commerce-developments-wto-mc13.

Joint press release on the Accession of the Republic of Korea to the Digital Economy Partnership Agreement (June 8, 2023), NEW ZEALAND MINISTRY OF FOREIGN AFFAIRS AND TRADE, https://www.mfat.govt.nz/en/media-and-resources/joint-press-release-on-the-accession-of-the-republic-of-korea-to-the-digital-economy-partnership-agreement/.

The Data Localization Debate in International Trade Law (June 22, 2020), IKIGAI LAW,https://www.ikigailaw.com/the-data-localization-debate-in-international-trade-law/#_ftn17.

Khasanova, Liliya & Katharin Tai (July 31, 2023), *An Authoritarian Approach to Digital Sovereignty? Russian and Chinese Data Localisation Models*, https://deliverypdf.ssrn.com/delivery.php?ID=808067068026071070068110001112066091035019070001075003096098086108083015105030002002106039102104013096111076012027070066115098126080022051012092119090071085080126030093028080092101002099075114026070101122092002123122030020006091102110000083100127085023&EXT=pdf&INDEX=TRUE.

doi:10.6342/NTU202402499

KPMG, *The Localisation of Russian Citizens' Personal Data: Compliance with the Russian Law on Personal Data* (September 2018), ADV-factsheet-localisation-of-russian-personnal-data-uk-LR.pdf (kpmg.com).

Kurth, Hunton Andrews, *India Releases Revised Non-Personal Data Framework*, NAT'L L. REV: HUNTON ANDREWS KURTH' PRIVACY AND CYBERSECURITY BLOG (January 15, 2021), https://www.natlawreview.com/Art./india-releases-revised-non-personal-data-framework.

LinkedIn blocked in Russia for violating provisions of "On the Procedure of Processing of Personal Data" Law of the Russian Federation, SPECHT & PARTNER, https://www.specht-partner.com/linkedin/.

Mak, Lauren & Chris Bluvshtein (March 18, 2024), *How to Unblock LinkedIn From Russia in 2024: A Full Guide*, VPNOVERVIEW, https://vpnoverview.com/unblocking/censorship/access-linkedin-russia/#:~:text=Is%20LinkedIn%20allowed%20in%20Russia,Russia%20in%20a%20few%20steps.

Manyika, James et alt. (February 24, 2016), *Digital Globalisation: The New Era of Global Flows*, MCKINSEY GLOB. INST., https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows.

MIKTA, *MIKTA e-commerce workshop reflections* (August 8, 2016), http://mikta.org/document/mikta-e-commerce-workshop-reflections/.

NATIONAL DATA SHARING AND ACCESSIBILITY POLICY, https://dst.gov.in/national-data-sharing-and-accessibility-policy-0.

NEW INITIATIVES ON ELECTRONIC COMMERCE, INVESTMENT FACILITATION AND MSME, https://www.wto.org/english/news_e/news17_e/minis_13dec17_e.htm.

NVIT (May 24, 2023), *Data Analytics in ICT*, LINKEDIN, https://www.linkedin.com/pulse/data-analytics-ict-nvitech.

Parkins, David (May. 6, 2017), *The World's Most Valuable Resource is No Longer Oil, but Data*, THE ECONOMIST, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

President Jean-Claude Juncker's State of the Union Address 2018 (September 12, 2018), EUROPEAN COMMITMENT, https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_18_5808.

doi:10.6342/NTU202402499

STORAGE OF PAYMENT SYSTEM DATA (April 6, 2018), https://www.rbi.org.in/commonperson/english/scripts/FAQs.aspx?Id=2995.

Russian Federation Federal Law on Personal Data, ONE TRUST DATA GUIDANCE, https://www.dataguidance.com/sites/default/files/en_20190809_russian_personal_data_federal_law_2.pd.

Russia's Leading Social Media Platform VK Has Been Expanding Fast, but at a Cost, INTELLINEWS (March 27, 2023), https://www.intellinews.com/russia-s-leading-social-media-platform-vk-has-been-expanding-fast-but-at-a-cost-274048//.

Russia's New Personal Data Localization Law Goes into Effect in September 2015, DUANE MORRIS (June 15, 2015), https://www.duanemorris.com/alerts/russia_new_personal_data_localization_law_into_effect_september_2015_0615.html(last visited Apr. 10, 2024).

Sayer, Peter (November 17, 2016), *LinkedIn blocked by Russian government*, PCWORLD, https://www.pcworld.com/article/411055/isps-ordered-to-block-linkedin-in-russia.html.

Schott, Jeffrey J., *Which Countries are in the CPTPP and RCEP Trade Agreements and Which Want in*, PETERSON INST. INT'L ECON., https://www.piie.com/research/piie-charts/which-countries-are-cptpp-and-rcep-trade-agreements-and-which-want.

South Africa Reserve Bank National Payment System Department, *Consultation Paper Processing of Payments in South Africa*, (November, 2018), https://financedocbox.com/Insurance/114473644-National-payment-systemdepartment-consultation-paper-processing-of-payments-in-south-africa.html.

Stratford, Timothy & Yan Luo (May 2, 2016), *3 Ways Cybersecurity Law in China is About to Change*, LAW360, https://www.cov.com/-/media/files/corporate/publications/2016/05/3_ways_cybersecurity_law_in_china_is_about_to_change.pdf.

TAPED A Dataset on Digital Trade Provisions, UNIV. LUCERNE, https://www.unilu.ch/en/faculties/faculty-of-law/professorships/burri-mira/research/taped/.

TAPED Codebook (2023/11/02), UNIV. LUCERNE, https://www.unilu.ch/en/faculties/faculty-of-law/professorships/burri-mira/research/taped/

doi:10.6342/NTU202402499

TAPED Dataset (2023/11/02), UNIV. LUCERNE, https://www.unilu.ch/en/faculties/faculty-of-law/professorships/burri-mira/research/taped/.

TPP Chapter Summary of Electronic Commerce, UNITED STATES TRADE REPRESENTATIVE, https://ustr.gov/sites/default/files/TPP-ChapterSummary-Electronic-Commerce.pdf.

The Digital Economy Partnership Agreement is a new initiative with Chile and Singapore, NEW ZEALAND MINISTRY OF FOREIGN AFFAIRS AND TRADE, https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement-depa/overview/.

The OJK Issues Regulation on Implementation of Insurance and Reinsurance Companies (January 19, 2017), GLOBAL BUSINESS GUIDE INDONESIA, , http://www.gbgindonesia.com/en/main/legal_updates/the_ojk_issues_regulation_on_implementation_of_insurance_and_reinsurance_companies.php.

The Transformative Power of Cloud Computing: A Glimpse into the Future (December 14, 2023), DIGITAL4BUSINESS, https://digital4business.eu/the-benefits-of-cloud-computing-for-smes/.

Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017), DIGICHINA (June 29, 2018) https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/.

UK-EU Trade and Cooperation Agreement Summary, GOV. UK, https://assets.publishing.service.gov.uk/media/602cf3dbd3bf7f031ce1360e/TCA_SUMMARY_PDF_V1-.pdf.

Understanding the WTO: The Organization Members and Observers, WORLD TRADE ORGANIZATION, https://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm.

Unleashing the Value of Data: Exploring Why Data is the New Gold (October 20, 2023), SECURITY PRIVACY, https://secureprivacy.ai/blog/significance-of-data-in-digital-era.

U.S. Chamber Letter: USMCA Now (Octomer 1, 2019), U.S. CHAMBER OF COMMERCE, https://www.uschamber.com/usmca.

U.N. CONF. ON TRADE & DEV., INVESTMENT AND THE DIGITAL ECONOMY xiii, WORLD INVESTMENT REPORT 2017 (2017), https://unctad.org/publication/world-investment-report-2017.

United States-Mexico-Canada Trade Fact Sheet: Modernizing NAFTA into a 21st Century Trade Agreement, UNITED STATES TRADE REPRESENTATIVE

doi:10.6342/NTU202402499

https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/fact-sheets/modernizing.

Wagner Aron (December 5, 2023), *The Future of Cloud Storage: Trends and Predictions, American Cloud*, AMERICAN CLOUD, https://americancloud.com/blog/the-future-of-cloud-storage-trends-and-predictions .

WHAT IS DATA, https://dataschools.education/about-data-literacy/what-is-data/.

WHAT IS THE WTO, https://www.wto.org/english/thewto_e/whatis_e/whatis_e.htm.

doi:10.6342/NTU202402499