STUDIA IURIS

Jogtudományi Tanulmányok / Journal of Legal Studies

2025. II. évfolyam 2. szám

Károli Gáspár Református Egyetem
Állam- és Jogtudományi Doktori Iskola

A folyóirat a Károli Gáspár Református Egyetem Állam- és Jogtudományi Doktori Iskolájának a közleménye. A szerkesztőség célja, hogy fiatal kutatók számára színvonalas tanulmányaik megjelentetése céljából méltó fórumot biztosítson.
A folyóirat közlésre befogad tanulmányokat hazai és külföldi szerzőktől – magyar, angol és német nyelven. A tudományos tanulmányok mellett kritikus, önálló véleményeket is tartalmazó könyvismertetések és beszámolók is helyet kapnak a lapban.
A beérkezett tanulmányokat két bíráló lektorálja szakmailag. Az idegen nyelvű tanulmányokat anyanyelvi lektor is javítja, nyelvtani és stilisztikai szempontból.
A folyóirat online verziója szabadon letölthető (open access).

Kiadó: Károli Gáspár Református Egyetem Állam- és Jogtudományi Doktori Iskola
Székhely: 1042 Budapest, Viola utca 2-4
Felelős Kiadó: Tóth J. Zoltán

A tipográfia és a nyomdai előkészítés: Csernák Krisztina (L'Harmattan) munkája
Nyomdai kivitelezés: Prime Rate Zrt., felelős vezető: Tomcsányi Péter

Honlap: https://ajk.kre.hu/index.php/jdi-kezdolap.html
E-mail: doktori.ajk@kre.hu
ISSN 3057-9058 (Print)
ISSN 3057-9392 (Online)
URL: KRE ÁJK - Studia Iuris
https://ajk.kre.hu/index.php/kiadvanyok/studia-iuris.html

DATA LOCALIZATION, SECURITY AND ECONOMIC GROWTH
ADATLOKALIZÁCIÓ, BIZTONSÁG ÉS GAZDASÁGI NÖVEKEDÉS

Ali Sanar Shareef[1]

ABSZTRAKT ■ Újonnan felfedezett értékük miatt az online adatok meghaladták a puszta emberi jogi státuszt, hiszen igen keresett árucikké váltak. Válaszul az országok megerősítették a jogalkotási intézkedéseiket az ilyen adatok szabályozására és ellenőrzésük megőrzésére. Gyakran nemzeti határaikon belülre korlátozzák az adatvédelmet, ez az álláspont ugyanakkor ellentmond a második világháború utáni nemzetközi mozgalomnak, amely a kereskedelmi akadályok lebontására irányul. Bár az országok úgy vélik, hogy az adatvédelmet érintő intézkedések a nemzetbiztonságot és a gazdasági érdekeket védik, nem valószínű, hogy a korlátozások hosszú távon fenntarthatóak lesznek. Ezért a szerző azt állítja, hogy ezek az intézkedések ellentmondanak a szolgáltatások szabad mozgásának elvének, és hosszú távon negatívan érintik a nemzetközi kereskedelmet.

Kulcsszavak: adatlokalizáció, WTO-egyezmények, szabad adatáramlás

ABSTRACT ■ Given its newfound value, online data has transcended its status as a mere human right to become a highly sought-after commodity. In response, countries have intensified legislative measures to regulate such data and retain control over it, often confining it within their national borders – a stance that contradicts the post-World War II international movement toward dismantling trade barriers. While countries believe these measures protect national security and economic interests, it is unlikely that such restrictions will be sustainable in the long term. Therefore, the author argues that these measures contradict the principle of free movement of services and, in the long run, will negatively impact international trade.

Keywords: data localization, WTO agreements, free flow of data

[1] PhD student, Doctoral School of Law and Political Sciences, Károli Gáspár University of the Reformed Church in Hungary.

1. Introduction

The advent rise of the Internet and technological advances have had a profound impact on global trade and the economy. Personal data is often referred to as the new oil of the internet and the new currency of the digital age.[2] Nearly half of global trade in services now relies on information and communications technology (ICT).[3] This development was initially expected to help the international community reduce trade barriers. However, data localization measures have undermined this expectation by restricting data transfers, thereby hampering the free movement of goods and services. Many countries have enacted laws that make it difficult to transfer personal data across borders under the guise of privacy and security. While these laws are not directly aimed at data localization, they effectively act as data localization measures by creating significant obstacles to data export.[4] The advancement of technologies, products, and services in recent decades has relied heavily on the unrestricted flow of data across borders. For companies to operate, innovate, and remain competitive in global markets, they must be able to move data.[5] Data localization measures fragment the World Wide Web, which was originally intended to facilitate the global exchange of information.[6]

The problem of the study lies in the enactment of laws requiring data localization and restricting data transfers. Countries believe that such measures will benefit their economies; however, it remains unclear whether these policies will have positive long-term effects. Therefore, it is crucial to ask: What is data localization? Does it contradict WTO principles? How do major powers such as the USA, China, and the EU approach it? What are the motives behind these laws, and what challenges do they pose?

This study aims to examine data localization laws, their violations of international trade law, and their effects on the free movement of goods and services, as well as the economies of the enacting states. To achieve this, the study is divided into five chapters, including an introduction and a conclusion. The second chapter explains the concept of data localization and evaluates it in light

[2] *National Board of Trade. No Transfer, No Trade: The Importance of Cross-Border Data Transfers for Companies Based in Sweden*. First edition. January 2014. ISBN: 978-91-86575-76-2. https://unctad.org/system/files/non-official-document/dtl_ict4d2016c01_Kommerskollegium_en.pdf (Accessed 15 February 2025).

[3] Ibid.

[4] Anupam Chander – Uyen P. Le: Breaking the Web: Data Localization vs. the Global Internet. *Emory Law Journal, Forthcoming, UC Davis Legal Studies Research Paper*, 2014 (378).

[5] National Board of Trade 2014, Ibid.

[6] Chander – Le 2014, 8.

of WTO regulations. The third chapter analyzes the EU, China, and the USA , which together account for a huge percentage of global trade. The fourth chapter explores the motives behind data localization laws and the criticisms they face.

The study adopts an analytical methodology, relying on formal sources such as laws and international treaties, as well as informal sources like books and academic articles.

2. What is data localization and does it hamper free international trade

2.1. The concept of data localization

It is difficult to define this term, as it lacks a universally accepted definition,[7] and its meaning varies depending on the context.[8] However, it refers to the requirement,[9] or the practice[10] of storing or processing[11] data within the territorial borders of a country. In other words, it involves keeping data locally to protect against leakage of personal information.[12]

There is a debate about what constitutes data localization: Some consider implicit measures such as restrictions on cross-border data flows to be forms of localization, while others emphasize explicit regulations that directly dictate where and how data is stored or processed within a jurisdiction.[13]

Despite the controversy surrounding this concept, there has been a global trend towards greater control over data, especially in the wake of the COVID-19 pandemic.[14] Many countries have adopted data localization legislations,[15] both

7 Chiara Del Giovane – Janos Ferencz – Javier López González: *The Nature, Evolution and Potential Implications of Data Localisation Measures*. OECD Trade Policy Papers 278, OECD Publishing, 2023.

8 Gargi Whorra: Data Localization: An Issue beyond Borders. *RGNUL Financial and Mercantile Law Review,* 2022 (43), 495-503.

9 Elaine Fahey: Does the EU's Digital Sovereignty Promote Localisation in Its Model Digital Trade Clauses? *European Papers*, 2023 (2), 503-511.

10 Jigyasa Singh: Data Localization. *Jus Corpus Law Journal*, 2022 (2), 495-503, 496.

11 Fahey 2023, 505.

12 Singh 2022, 496.

13 Del Giovane – Ferencz – González 2023, 5.

14 Wenxi Lu: Data Localization: From China and Beyond. *Indiana Journal of Global Legal Studies*, 2024 (1), 183-202, 184.

15 Ibid.

developed and developing countries.[16] In 2021, 92 data localization measures were implemented in 39 countries, with more than half of them emerging in the past five years.[17] By early 2023, nearly 100 data localization measures had been implemented across 40 countries, with over half of them introduced since 2015.[18] These legislations take different forms and seizes. In terms of the type of data, Data localization measures can be categorized into three main groups: The first is broad localization, which requires all categories of personal data to be stored locally within a country. The second is specific localization, which applies to specific categories of personal data and specific organizations, and mandates local storage of that data. The third is Combined localization, which focuses on specific categories of personal data but does not require local storage. Instead, the focus is on ensuring that data processing complies with specific legal requirements.[19] In terms of regulatory frameworks there are different categories of legislation, ranging from outright bans on the transfer of any type of data to targeted restrictions on data transfers in specific sectors.[20] Category 1 includes local storage requirements without prohibiting overseas storage or processing, such as UK Companies Act 2006,[21] Category 2 requires local storage and processing but allows international access or transfer under specific circumstances,[22] such as Australia's Electronic Health Records Act, which mandates local storage but allows overseas access in certain situations. Category 3 mandates local storage and processing but prohibits international transfer, except under specific authorizations. Examples include Indonesia's Regulation 71 (2019) and China's Cybersecurity Law.[23] Additionally, new Category 0 focuses on data access rather than location, such as Denmark's Accounting Act, which removed local storage requirements in favor of ensuring access for public authorities.[24]

16 Susannah Hodson: Applying WTO and FTA Disciplines to Data Localization Measures. *World Trade Review*, 2019 (4), 579-607, 580.

17 Fahey 2023, 505.

18 Del Giovane – Ferencz – González 2023, 3.

19 Singh 2022, 496.

20 Satori Cyber, Data Localization 101: The Essentials, https://satoricyber.com/cloud-data-governance/data-localization-101-the-essentials/#:~:text=GDPR%20Data%20Localization%20Requirements,-As%20was%20just&text=According%20to%20GDPR%2C%20businesses%20are,up%20for%20equal%20privacy%20protections (Accessed 15 February 2025).

21 United Kingdom, 2006. Companies Act 2006. Part 15, Chapter 2, section 388. legislation.gov.uk (Accessed 15 February 2025).

22 Benjamin Wong: Data Localization and ASEAN Economic Community. *Asian Journal of International Law*, 2020 (1), 158-180, 165.

23 Lu 2024, 183.

24 Del Giovane – Ferencz – González 2023, 7-11.

2.2. The WTO agreements and data localization

In their paper, Anupam Chander and Owen B. Lee argue that governments around the world are increasingly asserting control over the World Wide Web, fragmenting it. For example, Iran aims to create an internet free of Western influence and dissent, while Australia restricts the export of health data. Similarly, South Korea requires that map data be stored locally, and Vietnam requires local copies of all Vietnamese data. These measures are akin to the creation of "Schengen data zones", effectively blocking global services. The authors compare this trend to the non-tariff barriers of the last century, which have now resurfaced as digital firewalls, blocking international services.[25]

When the General Agreement on Trade in Services (GATS) was established in 1994, the Internet was still in its early stages, so it is not surprising that the GATS does not specifically address digital trade barriers,[26] however, such flows may still be captured by GATS' 'mode of supply 1' (cross-border trade) when data transfers enable cross-border provision of services.[27] Additionally, Article XXVIII(b) of the GATS covers the broad supply of services, including activities such as production and delivery. Cross-border data flows are critical to enabling services under Mode 1 commitments, such as e-commerce and online consulting. Restrictions on data flows could therefore conflict with these commitments, affecting global trade. Therefore, by considering the goals of GATS agreement as whole we can derive some protection against digital trade barriers, including data localization measures, that discriminate against foreign suppliers or limit market access in sectors to which countries have committed. Or at least these provisions are provided unconditionally, so there is nothing to prevent them to be applied on the data localization since the latter impedes international trade.

However, the lack of specific rules creates uncertainty about how the GATS Agreement will apply to data localization in disputes. Arbitration panels and the Appellate Body have succeeded in reducing this uncertainty to some extent by interpreting the GATS Agreement in a flexible and technology-neutral manner, assuming that commitments cover all modes of supply, including online services, unless a country specifically restricts this in its schedule. However, the ongoing deadlock in WTO negotiations has prevented such interpretations from being formally incorporated into the text of the agreement.[28]

[25] Chander – Le 2014, 1.

[26] Hodson 2019, 582.

[27] Svetlana Yakovleva: Personal data transfers in international trade and EU law: a tale of two 'necessities'. *The Journal of World Investment & Trade*, 2020 (6), 881-919.

[28] Hodson 2019, 582.

Hodson argues that (GATS) addresses data localization measures in two ways. First, digital technologies are included to the extent that they enable services, such as electronic payment systems, to be provided across borders. Second, certain data-related services, such as database management and data processing, are explicitly covered in countries' schedules of commitments, which set out their obligations regarding market access and national treatment of foreign service providers. These provisions ensure that digital services are subject to GATS rules unless specific limitations are specified in a country's commitments.[29]

However, even if there is uncertainty about whether data flows are explicitly covered under the WTO, a closer examination of its general objectives and framework suggests that data localization contradicts its fundamental goal of promoting open and unrestricted trade.

3. In Practice

There have been international efforts to limit or prohibit data localization. The article 19.2 of the United States-Mexico-Canada Agreement (USMCA),[30] the Article 14.13 of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP),[31] and the Article 201 of the EU-UK Trade and Cooperation Agreement (TCA)[32] prohibit requiring companies for locating computing facilities within the territory of one party as a condition of conducting business. While the USMCA and CRTPP focus on preventing mandatory data localization, the CRTPP also recognizes each party's regulatory needs regarding security and confidentiality. However, national security exceptions have allowed many governments to derogate from these rules, rendering these provisions limited, if not ineffective.

[29] Hodson 2019, 586.

[30] United States-Mexico-Canada Agreement, Chapter 19, Digital Trade. Signed July 1, 2020 (Accessed September 22, 2024). United States Trade Representative. Agreement between the United States of America, the United Mexican States, and Canada 7/1/20 Text | United States Trade Representative (ustr.gov) (Accessed 15 February 2025).

[31] Comprehensive and Progressive Agreement for Trans-Pacific Partnership. Signed February 4, 2016, Auckland, New Zealand, Australian Government Department of Foreign Affairs and Trade. https://www.treaties.mfat.govt.nz/search/details/t/3911 (Accessed 15 February 2025).

[32] Trade and Cooperation Agreement. Signed in December 30, 2020, provisionally applied in January 1, 2021, entered into force May 1, 2021. European Union and European Atomic Energy Community, and the United Kingdom of Great Britain and Northern Ireland.

Since these international frameworks are neither comprehensive nor universal, state practices have taken different approaches that do not necessarily align with the principles enshrined in these frameworks.

The USA, the EU, and China, which together account for 90% of global trade,[33] share many similarities in regulating data transfers, yet significant differences remain. Each has imposed restrictions on data transfers, though the nature and extent of these restrictions differ.

Privacy legislation in China has become increasingly complex, with a number of laws and regulations being introduced. These laws and regulations include strict rules on the transfer of personal data stored in China to foreign entities, with the aim of protecting the privacy rights of Chinese data subjects.[34] While privacy rights are addressed, the primary purpose of restricting data transfers is to protect national security interests.[35] The departures of LinkedIn and Yahoo from China in 2021 highlight the challenges of complying with China's stringent data localization laws, although the specific reasons for their departures remain unclear.[36]

Unlike the EU, China lacks a unified data protection framework. Instead, its personal information protection system is based on three main laws: The Personal Information Protection Law (PIPL), the Cybersecurity Law (CSL), and the Data

[33] Lauren Kyger: *Data localization and other barriers to digital trade*. Hinrich Foundation (accessed august 8, 2024), https://www.hinrichfoundation.com/research/tradevistas/digital/data-localization/.

[34] Andrea Tang: Cross-Border Data Transfer and Data Localization Requirements in China. *ISACA 2021*, https://www.isaca.org/resources/news-and-trends/industry-news/2021/cross-border-data-transfer-and-data-localization-requirements-in-china?gad_source=1&gclid=EAIaIQobChMIxtPloKPriQMVgoKDBx0jSCjBEAAYAiAAEgJGAPD_BwE#8.

[35] Look for example: Data Security Law of the People's Republic of China, in Article 25 implements export controls for certain types of data to safeguard national security, Article 10 prohibits, transmitting or engaging in the processing of personal information that endangers the national security or public interests. Also, Article 1 of "Outbound Data Transfer Security Assessment Measures" provides: in order to regulate outbound data transfer activities, safeguard national security these Measures are formulated. Article 8 evaluates the potential risks associated with outbound data transfers, focusing on their impact on national security, public interest, and the legal rights and interests of individuals and organizations. And article 1 of Regulations on Network Data Security Management? (Please check the sentence marked with yellow, for me it is had to understand, also the last sentence, about Article 1.) I used ellipses before and after the quoted phrase to indicate that the excerpt is part of a longer sentence, with words omitted at both the beginning and end. This preserves the original meaning while focusing on the most relevant portion of the text.

[36] Lu 2024, 183.

Security Law (DSL).[37] In addition to these, there are specific laws regulating data transfers, which provide detailed guidelines and restrictions, such as Regulations on Network Data Security Management,[38] Regulations on the Security Protection of Critical Information Infrastructure,[39] State Administration for Market Regulation and National Standardization Administration.[40] Furthermore, various provisions in different Chinese laws impose restrictions on the transfer of data outside of China.[41]

The Article 4 of the "Outbound Data Transfer Security Assessment Measures"[42] requires data handlers that they must apply for an outbound data transfer security assessment if they provide important data abroad, or if critical information infrastructure operators or data operators have transferred the personal information of more than 1 million individuals abroad, or if they have transferred more than 100,000 personal information of individuals or more than 10,000 sensitive personal information of individuals since 1st January of the previous year. In addition, a security assessment is required in other circumstances determined

37 DLA Piper: Data Protection Laws of the World: China. 2024, www.dlapiperdataprotection.com (Accessed 13 January 2025).

38 State Council of the People's Republic of China: Regulations on Network Data Security Management. Order No. 790, adopted August 30, 2024, and effective January 1, 2025, Article 5, https://www.gov.cn/zhengce/content/202409/content_6977766.htm (Accessed 13 January 2025).

39 Regulations on the Security Protection of Critical Information Infrastructure: Order No. 745, adopted April 27, 2021, and effective September 1, 2021 (Accessed December 6, 2024). https://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm (Accessed 13 January 2025).

40 State Administration for Market Regulation and National Standardization Administration: https://www.chinesestandard.net/PDF/English.aspx/GBT43697-2024 (Accessed 15 February 2025).

41 Look for example: Regulation on the Administration of Credit Investigation Industry, Order No. 631. Adopted at the 228th executive meeting of the State Council, December 26, 2012. The Regulation shall come into force on March 15, 2013. (2013) http://camlmac.pbc.gov.cn/en/3688253/3689006/3858830/index.html (Accessed 13 January 2025). PRC Law on the Protection of State Secrets. Promulgated February 27, 2024, to take effect on May 1, 2024 (Accessed November 20, 2024). Articles 28 and 57. https://www.chinalawtranslate.com/en/secrets-law-2024/ (Accessed 13 January 2025). Notice of the People's Bank of China on Protecting Personal Financial Information by Banking Financial Institutions. People's Bank of China. Article 6. Last modified 2011 (Accessed November 20, 2024), http://www.pbc.gov.cn/en/3688253/3689009/3788477/3911512/index.html.

42 Digichina, Outbound Data Transfer Security Assessment Measures, Self Assessments and CAC Review for Cross-Border Data Transfers. Take Effect Sept. 1, 2022. https://digichina.stanford.edu/work/translation-outbound-data-transfer-security-assessment-measures-effective-sept-1-2022/ (Accessed 13 January 2025).

by the State Cybersecurity and Information department.[43] This will leave the list open to further restrictions and giving the department discretionary power that allows it to determine requirements without clear boundaries. Additionally, the security assessment measures do not explain how the personal information thresholds (1 million, 100,000, and 10,000 individuals) are calculated. It is uncertain whether these thresholds apply to all personal information processed by an entity, regardless of information systems, business functions, or categories of data subjects.[44]

When examining EU policy, it is clear that the free movement of trade and services is of paramount importance to the functioning of the Union. Article 56 of the Treaty on the Functioning of the European Union prohibits restrictions on the provision of services across Member States.

The GDPR, as a successor to the Data Protection Directive, is a comprehensive personal data protection law that applies across the European Union, appears to extend these principles beyond EU Member States. It defines its subject matter and objectives as two main points: respect for personal data and recognition of the necessity of data flows for international trade and cooperation. However, achieving this balance is not an easy task for the EU, as it seeks to reconcile the seemingly conflicting goals of protecting personal rights and enabling economic activity and free data flows. The EU recognised these challenges early on and has built flexibility into its legal framework to ensure that the protection of personal rights does not unduly impede economic endeavors or cross-border data flows. This flexibility is enshrined in Article 52(2) of the EU Charter of Fundamental Rights, which states that the rights recognised in the Charter and set out in the Treaties must be exercised under the conditions and within the limits set out in those Treaties.[45]

Under the GDPR, cross-border data transfers are regulated with several possible grounds for legitimacy. Article 45 allows personal data to be transferred to a third country if the European Commission has determined that the country ensures an adequate level of protection. Alternatively, under Article 46, appropriate safeguards such as binding corporate rules, standard contractual clauses, codes of conduct, or certifications may be used, provided they guarantee

[43] Ibid.

[44] Kate Yin – Gil Zhang – Yanhua Lin – Derrick Zhao: China Finalized Its Security Assessment Mechanism for Cross-border Data Transfer. Fangda Partners, https://www.fangdalaw.com/wp-content/uploads/2022/07/China-finalized-its-security-assessment-mechanism-for-cross-border-data-transfer.pdf (Accessed 13 January 2025).

[45] European Union, Charter of Fundamental Rights of the European Union (2012/C 326/02). Official Journal of the European Union C 326, 26 October 2012. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT (Accessed 13 January 2025).

enforceable rights for data subjects and legal remedies. In contrast, Article 38 of China's PIPL[46] imposes more stringent conditions for transferring personal information outside China. Personal information processors must either pass a security assessment, obtain a personal information protection certificate, sign a standard contract, or comply with other legal or regulatory provisions specified by the state cybersecurity authority.

China regards data transfer a matter of national security, making the executive's decision final and non-appealable, and there is no recourse to the courts. Appeals are limited to the same body that made the initial decision, with no higher institution available for review. According to Article 13, data operators who disagree with the outcome of an assessment may request a review from the National Cybersecurity and Information Administration within 15 working days. The review decision is final, making it unlikely that the outcome will change. In contrast, the GDPR provides more comprehensive legal remedies. Under Article 78, individuals can file a complaint with a supervisory authority, and if they are dissatisfied with the outcome, they can seek judicial redress in the courts, ensuring external and independent review of decisions.

3.1. Non-personal data

For non-personal information, Article 3 of the Regulations on Promoting and Regulating the Cross-border Data Flow allows exemptions for certain cross-border activities that do not involve personal information or important data, such as "international trade, cross-border transportation, academic cooperation, cross-border production and manufacturing, and cross-border marketing". By contrast, the EU takes a different approach to non-personal data, with a broader framework and narrower restrictions. The European Data Governance Act,[47] the

[46] Personal Information Protection Law of the People's Republic of China: adopted at the 30th Meeting of the Standing Committee of the 13th National People's Congress on August 20, 2021, effective November 1, 2021. https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/ (Unofficial English translation, Accessed 13 January 2025).

[47] European Commission, European Data Governance Act. The act entered into force on June 23, 2022, with full applicability from September 2023. https://digital-strategy.ec.europa.eu/en/policies/data-governance-act (Accessed 13 January 2025).

Data Act[48] and the upcoming European Health Data Space[49] impose restrictions on the transfer of non-personal data outside the EU. While these restrictions may appear to be primarily aimed at protecting non-personal data, they also aim to prevent individuals from being re-identified through such data.[50]

3.2. United States

The USA does not have a comprehensive data protection law equivalent to the GDPR in Europe. Instead, it relies on a patchwork of sector-specific or state laws to address data protection.

The U.S. communicates its policies and stance on data localization through international governance bodies and trade agreements, such as the United States-Mexico-Canada Agreement, which prohibits data localization and promotes the free flow of data among the member countries.[51] However, certain data localization or residency laws may mandate the storage of personal data within the country.[52] Several data localization requirements have been proposed or implemented, primarily centered on public procurement.[53] Recently, the U.S. advocated for financial services data to be exempt from the Trans-Pacific Partnership's rules that barred countries from imposing barriers to data flows. However, after the agreement was concluded, the U.S. aimed to narrow the scope of this exemption through bilateral talks and provisions in ongoing Trade in Services Agreement

48 European Union, Regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data and Amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). European Union, November 15, 2023, https://data.consilium.europa.eu/doc/document/PE-49-2023-INIT/en/pdf (Accessed 13 January 2025).

49 Inside Privacy, Leaked Draft Version of the European Health Data Space Regulation, 2022. https://www.insideprivacy.com/international/european-union/leaked-draft-version-of-the-european-health-data-space-regulation/ (Accessed 13 January 2025).

50 Kristof Van Quathem – Anna Oberschelp de Meneses: EU Rules Restricting the International Transfers of Non-Personal Data. Inside Privacy (2024), https://www.insideprivacy.com/health-privacy/eu-rules-restricting-the-international-transfers-of-non-personal-data/.

51 Global Regulatory Insights: Does the USA Have Any Provisions for Data Localization or Specific Storage Requirements for Personal Data? https://globalregulatoryinsights.com/frequent-search/does-the-usa-have-any-provisions-for-data-localization-or-specific-storage-requirements-for-personal-data/ (Accessed 13 January 2025).

52 Ibid.

53 Nigel Cory: Cross Border Data Flows. Where are the Barriers and What do They Cost? In: *Information Technology and Innovation Foundation*, 2017, https://itif.org/publications/2017/05/01/crossborder-data-flows-where-are-barriers-and-what-do-they-cost (Accessed 13 January 2025).

negotiations.[54] Data localization requirements in the United States are influenced by various factors, including national security laws, and its approach to data localization seeks to balance national security and data protection with the free flow of information for economic and security purposes.[55] Biden's executive order cites national security, foreign policy, privacy protections, and other human rights and freedoms as reasons behind its issuance. However, the law is only applicable against certain countries.[56]

Data localization requirements in the United States are governed by a combination of federal regulations and state-level legislative efforts, each emphasizing the protection of sensitive information within U.S. jurisdictional boundaries. At the federal level, Internal Revenue Service Publication 1075[57] mandates that Federal Tax Information (FTI) must be accessed, processed, stored, and transmitted exclusively within the United States, including its territories, embassies, and military installations. This regulation explicitly prohibits foreign remote maintenance, call centers, or help desks from handling FTI. Similarly, the Defense Acquisition Regulations System (239.7602–2)[58] requires cloud computing service providers to maintain all government data within the 50 states, the District of Columbia, or outlying U.S. areas, unless explicitly authorized by a designated official. This aligns with the City of Los Angeles' contract with Google, which stipulates that email and Google Message Discovery data must remain within the continental United States, as outlined in the Statement of Work (Appendix B, Section 1.1.10.4).[59]

54 Ibid.

55 Global Regulatory Insights.

56 The White House: Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern. Issued by President Joseph R. Biden. Published February 28, 2024. https://www.whitehouse.gov/briefing-room/presidential-actions/2024/02/28/executive-order-on-preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related-data-by-countries-of-concern/ (Accessed 13 January 2025).

57 Internal Revenue Service: Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information, Rev. 11-2021, 57, https://www.irs.gov/pub/irs-pdf/p1075.pdf (Accessed 13 January 2025).

58 Defense Acquisition Regulations System: Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services. Federal Register 80, no. 165, 2015, https://www.govinfo.gov/content/pkg/FR-2015-08-26/pdf/2015-20870.pdf (Accessed 13 January 2025).

59 City of Los Angeles: Supplemental Report - Information Technology Agency Request to Enter into a Contract with Computer Science Corporation for the Replacement of the City's E-Mail System. Inter-Departmental Correspondence, October 7, 2009 https://clkrep.lacity.org/onlinedocs/2009/09-1714_rpt_cao_10-7-09.pdf (Accessed 13 January 2025).

At the state level, several bills introduced in the early 2000s sought to impose similar restrictions, particularly targeting call centers and the overseas transfer of personal data. For instance, Missouri House Bill No. 1497 (2004)[60] prohibits state contracts with foreign-based call centers and bans the transfer of financial, credit, or identifying information to foreign countries without express written consent (Section 1, Subsection 3). Similar provisions are found in Kansas House Bill No. 2810 (2004), Washington House Bill No. 3186 (2004), and Tennessee Senate Bill No. 3492 (2004), all of which restrict the use of foreign call centers for state contracts and require operators to disclose their location upon request. Ohio House Bill No. 459 (2004) also aimed to prohibit state contract work from being performed outside the U.S. and required consumer consent for data transfers overseas, though it never became law.[61]

While the USA doesn't not have comprehensive provisions on cross-border data transfers like EU and Chine. However, it does implement measures with some similarities. Biden's executive order provides exceptions to restrictions on data transfer, as it does not prohibit U.S. individuals or entities from conducting commercial transactions or exchanging financial and other data as part of selling goods and services to entities in countries of concern.[62]

Section 202.301 of the Biden's order categorizes types of data similarly to China's approach, as it prohibits covered data transactions – involving access to government-related data or bulk U.S. sensitive personal data – from being transferred to countries of concern or covered persons.[63]

60 National Foundation for American Policy. State Legislation on Global Sourcing, 2004 - Table Tracking State and Federal Global Sourcing Legislation 2004, https://www.nfap.com/researchactivities/globalsourcing/appendix.aspx (Accessed 13 January 2025).

61 National Foundation for American Policy: State Legislation on Global Sourcing, Table Tracking State and Federal Global Sourcing Legislation. 2004, https://www.nfap.com/researchactivities/globalsourcing/appendix.aspx (Accessed 13 January 2025).

62 The White House: Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern, Ibid.

63 Department of Justice, National Security Division: NSD 104 - Data Security - 1124-AA01 - Final Rule: Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons. Final Rule, February 28, 2024. Washington, DC: U.S. Department of Justice. https://www.justice.gov/nsd/media/1382521/dl (Accessed 13 January 2025).

4. Motives and criticism

Although there is limited empirical data to accurately measure costs, data localization is widely seen as a major hurdle for companies relying on digital technology in modern commerce.[64]

There are many factors behind data localizations, such as enhancing national security, supporting local economies, and protecting human rights.[65] The transfer of data across borders raises concerning the potential leakage of personal information, especially foreign governments or organizations.[66] By keeping sensitive data within their borders, they aim to prevent hostile governments from easily accessing or collecting such information. For example, South Korea requires companies to store map data within the country due to security concerns related to North Korea. Similarly, on 14th August 2020, the United States ordered ByteDance, the parent company of TikTok, to relinquish all rights and interests in data obtained from American users, due to concerns about foreign misuse. Another reason for data localization is the fear of foreign digital colonization, as countries fear over-reliance on powerful multinational tech companies, especially large countries like the United States.[67]

Storing data locally can stimulate the local economy by creating jobs, especially in sectors such as e-commerce and financial services. When data is collected and processed locally, it requires local manpower to manage the data, drive growth in related industries, and support the development of local expertise and infrastructure.[68] Data localization mandates can boost local innovation by allowing local companies to fill gaps left by departing multinationals. In China, companies like Baidu and Weibo have thrived after the exits of Google and Twitter, expanding into advanced industries. They also boost local economies by creating jobs and attracting foreign investment, as seen with Apple's $1 billion data center in China and the construction of new data centers in Europe by tech giants like Microsoft and Amazon to comply with regulations.[69]

64 Hodson 2019, 580.
65 Lu 2024, 184.
66 Singh 2022, 497.
67 Lu 2024, 183.
68 Singh 2022, 497.
69 Lu 2024, 188.

4.1. Criticism

While countries assume that data localization protect their national security and promote economic interests, the reality does not always align with these goals. In his book Anupam Chander argues that Simply localizing data does not eliminate surveillance; for example, a significant portion of surveillance in the United States occurs outside its borders. In addition, the use of malware enables foreign agencies to infiltrate data systems, bypassing local security measures and firewalls. This renders efforts to contain data within borders largely ineffective.[70] Many academics criticize data localization, highlighting its negative effects such as weakening data security, increasing business costs, stifling industry growth, enabling government surveillance, and threatening Internet functionality.[71] Data localization can weaken security by forcing companies to rely on less secure local services, making them easier targets for foreign surveillance. It also centralizes data, making it more vulnerable to focused surveillance efforts by foreign agencies.[72] Pranesh Prakash, policy director at the Center for Internet & Society, advocates for decentralized, end-to-end encrypted services as the best solution. These services ensure that data is not stored in a single central location, enhancing security and privacy.[73]

Some experts argue that data localization initiatives may focus more on economic protection than on enhancing data privacy. By requiring data to be stored or processed locally, countries may aim to stimulate their domestic technology industries or boost their digital economies.[74] However, the actual impact of these measures remains unclear.

Data localization often hinders trade in services and impedes economic integration.[75] Critics of data localization measures argue that, rather than boosting domestic industries, these policies could stifle economic growth. They highlight issues such as reduced access to foreign markets and increased regulatory uncertainty, which can deter investment. Economists have compared data

70 Chander – Le 2014, 28-30.
71 Wong 2020, 159.
72 Chander – Le 2014, 28-30.
73 Dharmakumar: India's Internet Privacy Woes. *Forbes India*, 2013, https://www.forbesindia.com/article/checkin/indias-internet-privacy-woes/35971/1#ixzz2r0zriZTF (Accessed 13 January 2025).
74 Bret Cohen – Britanie Hall – Charlie Wood: Data Localization Laws and Their Impact on Privacy, Data Security and the Global Economy. 2017. https://research.ebsco.com/c/xxk6ow/viewer/html/xegxhu5ex5 (Accessed 13 January 2025).
75 Wong 2020, 159.

localization to import substitution, where companies aiming to enter domestic markets must invest in storing or processing data locally instead of utilizing international services.[76] These policies often make operations more complex, often leading to forced data localization. As a result, when a foreign company seeks to provide IT services in certain countries, such as India, it is often required to establish local partnerships.[77]

A study by the Swedish National Trade Board confirms that trade is impossible without data transfer between locations.[78] Some see data protection as an issue limited to the tech industry, but its impact extends across many sectors of the economy. And since almost all modern businesses rely on data-driven innovation, these protectionist measures could ultimately be detrimental.[79]

Additionally, data localization, which is considered a type of restriction on the free flow of trade, runs counter to reduction of trade barriers, which is one of the most important means of encouraging global commerce. The world trade organization (WTO),[80] and other regional frameworks such as Treaty on European Union (TEU) and Treaty on the Functioning of the European Union (TFEU)[81] have sought to reduce such barriers.[82] These principles extend to the free flow of data across borders, which is crucial for the global economy, allowing

76 Cohen – Hall – Wood, Ibid.

77 Satori Cyber.

78 National Board of Trade 2014, 23.

79 Cory 2017, 1.

80 Data localization requirements conflict with WTO principles by imposing restrictions on cross-border data flows, which could limit the number of service suppliers, service transactions, and foreign capital participation. These measures violate Article XVI of the General Agreement on Trade in Services, which prohibits such restrictions unless specified in a Member's Schedule. In addition, Article XVII provides for equal treatment of foreign and domestic service suppliers, which data localization undermines by harming foreign suppliers. World Trade Organization (WTO). "General Agreement on Trade in Services (GATS)" Marrakesh Agreement Establishing the World Trade Organization, 15 April 1994. https://www.worldtradelaw.net/document.php?id=uragreements/gats.pdf&mode=download#:~:text=For%20the%20purposes%20of%20this%20Agreement,%20trade%20in%20services%20is (Accessed 13 January 2025). Wong argues that, although the implementation of WTO rules may not explicitly oppose data localization, the broader WTO framework could accommodate it: Wong 2020, 165.

81 Article 3(3) of the Treaty on European Union (TEU) obliges the EU to create an internal market. Article 26 of Treaty on the Functioning of the European Union (TFEU) states that the EU shall adopt the measures necessary to create or ensure the proper functioning of such an internal market. Article 49 of the TFEU guarantees freedom of establishment, prohibiting restrictions on individuals from one EU Member State from establishing companies in another Member State, and Article 56 guarantees freedom to provide services, prohibiting restrictions on the provision of services across Member States.

82 World Trade Organization: Principles of the Trading System. https://www.wto.org/english/thewto_e/whatis_e/tif_e/fact2_e.htm (Accessed 13 January 2025).

businesses to operate internationally and giving consumers access to global markets. However, data localization is considered a barrier to this flow.

Therefore, contrary to claims of economic benefits, the opposite may be true. Free trade between countries and the removal of barriers tend to be more beneficial to economic growth. While these purported benefits of data localization may seem promising in the short term, it is unclear what long-term benefits they offer. With the rapid pace of technological development driving new regulations, the future of the free flow of data, among other concerns, remains unclear. It may be too early to predict the consequences, and the coming years will reveal how these regulations will impact global data practices and their side effects on other aspects, particularly free trade.

Moreover, data localization may have a negative impact on privacy, as governments may seek to control the data of their citizens, especially opposition activists, in order to monitor their activities. This suggests that the original intent is reversed, and that data localization violates privacy rather than protecting it.

In previous reports (A/HRC/17/27 and A/66/290), the Special Rapporteur examined the transformative impact of the Internet on individuals' ability to exercise their right to freedom of opinion and expression. He also raised concerns about various State-imposed measures that restrict the flow of information online and highlighted the insufficient protection of the right to privacy in the digital sphere.

5. Conclusion

After World War II, the international community sought to remove barriers to free trade, and to a large extent, they succeeded. However, technological advancements have introduced new challenges. Data, often considered the "oil" of the modern technological era, needs to be transferred across borders. Restricting such transfers undermines the free flow of services. Data localization, which refers to the requirement to store data within the borders of a particular country, is one such restriction. This can be seen as a violation of the principle of free flow of services enshrined in the WTO. Even if there is debate about whether data flows explicitly fall under this principle, an examination of the general objectives and framework of the WTO suggests that data localization contradicts its core goals of promoting open and barrier-free trade.

Furthermore, the adoption of such measure by the EU, the USA, and China, which together account for a large percentage of global business, could further exacerbate the situation. And though there is varying degrees between these

legislations, the localizations requirements are there and can have a profound impact on the free flow of data.

Additionally, while countries argue that data localization provides economic benefits and enhances national security, this may hold true in the short term. However, in the long run, its negative economic impacts remain uncertain, as no country can be entirely self-sufficient – cooperation and trade are essential. Moreover, data localization raises concerns about privacy and human rights, as it grants governments greater access to their citizens' data, particularly affecting activists.

Recommendations:

- The development of new, comprehensive, and binding international rules on data protection and localization.
- These rules should emphasize conditional transfers of data based on strong data protection safeguards, rather than outright prohibitions on cross-border data flows.
- Easing the burden on businesses: when implementing data localization for necessary security reasons, governments should work to reduce the financial and operational burden on businesses. This can be done by offering incentives such as tax breaks, fee waivers, or subsidies to offset compliance costs. By doing so, countries can ensure that businesses, especially small and medium-sized businesses, are not disproportionately impacted by these regulations, helping to maintain economic competitiveness.
- It may be considered prudent to amend the WTO framework to explicitly include provisions on data flows, thereby eliminating any ambiguity regarding their coverage.

Bibliography

Anupam Chander – Uyen P. Le: Breaking the Web: Data Localization vs. the Global Internet. *Emory Law Journal, Forthcoming, UC Davis Legal Studies Research Paper*, 2014 (378).

Bret Cohen – Britanie Hall – Charlie Wood: Data Localization Laws and Their Impact on Privacy, Data Security and the Global Economy. 2017, https://research.ebsco.com/c/xxk6ow/viewer/html/xegxhu5ex5.

Nigel Cory: Cross Border Data Flows. Where are the Barriers and What do They Cost? In: *Information Technology and Innovation Foundation*, 2017, https://itif.org/publications/2017/05/01/crossborder-data-flows-where-are-barriers-and-what-do-they-cost.

Elaine Fahey: Does the EU's Digital Sovereignty Promote Localisation in Its Model Digital Trade Clauses? *European Papers*, 2023 (2), 503-511.

Chiara Del Giovane – Janos Ferencz – Javier López González: *The Nature, Evolution and Potential Implications of Data Localisation Measures*. OECD Trade Policy Papers 278, OECD Publishing, 2023.

Susannah Hodson: Applying WTO and FTA Disciplines to Data Localization Measures. *World Trade Review*, 2019 (4), 579-607.

Lauren Kyger: *Data localization and other barriers to digital trade*. Hinrich Foundation. https://www.hinrichfoundation.com/research/tradevistas/digital/data-localization/.

Wenxi Lu: Data Localization: From China and Beyond. *Indiana Journal of Global Legal Studies*, 2024 (1), 183-202.

Jigyasa Singh: Data Localization. *Jus Corpus Law Journal*, 2022 (2), 495-503.

Andrea Tang: Cross-Border Data Transfer and Data Localization Requirements in China. *ISACA 2021*, https://www.isaca.org/resources/news-and-trends/industry-news/2021/cross-border-data-transfer-and-data-localization-requirements-in-china?gad_source=1&gclid=EAIaIQobChMIxtPloKPriQMVgoKDBx0jSCjBEAAYAiAAEgJGAPD_BwE#8.

Kristof Van Quathem – Anna Oberschelp de Meneses: EU Rules Restricting the International Transfers of Non-Personal Data. Inside Privacy (2024), https://www.insideprivacy.com/health-privacy/eu-rules-restricting-the-international-transfers-of-non-personal-data/.

Gargi Whorra: Data Localization: An Issue beyond Borders. *RGNUL Financial and Mercantile Law Review,* 2022 (43), 495-503.

Benjamin Wong: Data Localization and ASEAN Economic Community. *Asian Journal of International Law*, 2020 (1), 158-180.

Svetlana Yakovleva: Personal data transfers in international trade and EU law: a tale of two 'necessities'. *The Journal of World Investment & Trade*, 2020 (6), 881-919.

Kate Yin – Gil Zhang – Yanhua Lin – Derrick Zhao: China Finalized Its Security Assessment Mechanism for Cross-border Data Transfer. Fangda Partners, https://www.fangdalaw.com/wp-content/uploads/2022/07/China-finalized-its-security-assessment-mechanism-for-cross-border-data-transfer.pdf.