JOURNAL OF JURISPRUSDENCE, INTERNATIONAL LAW AND CONTEMPORARY LEGAL ISSUES
Rivers State University, Faculty of Law *ISSN: 1115 5167 Vol.18 Issue.2, August 2024*

BALANCING DATA LOCALISATION AND REGIONAL / INTERNATIONAL TRADE OBLIGATIONS IN DATA SOVEREIGNTY IN NIGERIA'S DIGITAL ECONOMY

By

Abraham Ebini*
Alasia, Joyce Ibiso**

Abstract
Data localization is a growing trend around the world, as governments seek to protect personal data and national sovereignty in the digital age. However, data localization measures can also hinder cross-border trade and economic growth. Nigeria is facing this challenge as it seeks to promote its digital economy. This paper examines the impact of data localization on international trade obligations in the context of Nigeria's digital economy. The paper finds that Nigeria's data localization measures may conflict with its obligations under the World Trade Organization's General Agreement on Trade in Services (GATS) and the African Continental Free Trade Area (AfCFTA). These agreements prohibit measures that restrict the free flow of data across borders. The paper also finds that data localization can increase operational costs for businesses and stifle innovation. The paper concludes that Nigeria must find a balance between data sovereignty and trade facilitation to ensure the full benefits of the digital economy are realized. The paper recommends that Nigeria adopt a data-driven approach to policymaking, conduct thorough impact assessments, and engage in active dialogue with stakeholders. The paper also recommends that Nigeria strengthen its cybersecurity infrastructure and promote digital literacy among its citizens. By implementing these recommendations, Nigeria can create a data localization framework that is balanced, transparent, and effective. This framework will help to protect personal data and national sovereignty while also facilitating trade and economic growth in the digital economy.
Keywords: *Data Localisation, Digital Economy, Nigeria, Trade facilitation.*

1.0 Introduction

The digital era has ushered in unprecedented advancements in technology, leading to an exponential growth in data generation and consumption.[1]This transformation has profound implications for national sovereignty, particularly in relation to the management and control of data.[3] Data sovereignty refers to the authority of a country to govern and regulate data within its jurisdiction,[1] ensuring that it is protected from unauthorized access or misuse.[2] As data becomes a strategic asset for nations, the need to establish clear frameworks for data localization has become increasingly apparent.

* LL.B (Hons), LL.M (in view) – Faculty of Law, Rivers State University, Port Harcourt, Rivers State, Nigeria Email: abraham.ebini@ust.edu.ng
** LL.B (Hons), L.B, LL.M (in view) – Faculty of Law, Rivers State University
Ibiso.alasia@ust.edu.ng
[1] Cristobal R P and Schuilenburg, L, 'Data sovereignty: Conceptualization, institutionalization, and empirical evidence' [2021] (28)(4) *Review of International Political Economy* 857-886.
[2] Fisher E H and others, *Research Handbook on Digital Labour and Work* (Edward Elgar Publishing 2022) 327.

As stated by Bosun Tijani, the Minister of Communications and Digital Economy of Nigeria, the ICT sector accounts for approximately 13 to 18% of the country's Gross Domestic Product (GDP). Specifically, in the fourth quarter of 2023, the sector contributed around 16.6% to the GDP. The digital economy of Nigeria achieved a revenue of $5.49 billion in 2019. Furthermore, projections indicate that this sector has the potential to generate up to $18.3 billion by 2026.[3] While developed nations like the United States, the United Kingdom, Germany and Japan have long been at the forefront of digital advancements, developing countries, including Nigeria, have increasingly recognised the need to integrate digital technology into their economic restructuring.[4]

The Nigerian government has taken steps to foster the country's digital economy. This includes renaming the Federal Ministry of Communications to the Federal Ministry of Communications and Digital Economy, as well as introducing economic policies and investments aimed at developing the necessary information and communications technology (ICT) capacity and infrastructure.[5] Nigeria's Economic Recovery and Growth Plan 2017–2020 and the National Digital Economy Policy and Strategy 2020-2030 have further underscored the government's commitment to harnessing the benefits of a digital economy.[6]

Data localization, the requirement for data to be stored or processed within a country's borders, has become a common strategy for safeguarding data sovereignty[7] However, this practice can create barriers to international trade, as it restricts the flow of data across borders, potentially hindering economic growth and innovation.[8] International obligations under agreements such as the World Trade Organization's General Agreement on Trade in Services (GATS) prohibit measures that restrict the trade in services, including data transmission.[9] This has raised concerns about the compatibility of data localization policies with Nigeria's trade obligations.

Nigeria, a leading economy in Africa, is rapidly adopting digital technologies and generating vast amounts of data.[10] Despite the recognition of the importance of data sovereignty, the country's data protection framework is still evolving. The Nigerian Data Protection Act (NDPA) 2023 is a legal framework dedicated to protection of data privacy while the Nigeria Data Protection Regulation

[3] Samson Akintaro, 'Nigeria's digital economy to generate $18.3 billion by 2026 – Bosun Tijani' (2024) <https://nairametrics.com/2024/07/10/nigerias-digital-economy-to-generate-18-3-billion-by-2026-bosun-tijani/> accessed 28 November 2024.
[4] *Ibid.*
[5] Federal Ministry of Communications and Digital Economy, 'National Digital Economy Policy and Strategy (2020-2030)' <https://www.ncc.gov.ng/docman-main/industry-statistics/policies-reports/883-national-digital-economy-policy-and-strategy/file> accessed 23 November 2024.
[6] The World Bank, Nigeria Digital Economy Diagnostic: A Plan for Building Nigeria's Inclusive Digital Future' <https://www.worldbank.org/en/country/nigeria/publication/nigeria-digital-economy-diagnostic-a-plan-for-building-nigerias-inclusive-digital-future> accessed 20 October 2024.
[7] Richard D Taylor, ''Data localization': The internet in the balance' [2020] (44)(8) *Telecommunications Policy* 78-92.
[8] European Data Protection Board, 'Guidelines 05/2020 on the Territorial Scope of the GDPR, Art. 3 (territorial scope)'(2020 <https://edpb.europa.eu/en/publications/guidelines/guidelines-052020territorial-scope-gdpr-art-3-territorial-scope_en> accessed 12 October 2024.
[9] World Trade Organization General Agreement on Trade in Services (GATS) 1994
[10] Rack Centre, 'Nigeria's Digital Transformation and AI-Ready Data Centres: Rack Centre, Leading the Charge' (2024) <https://techpoint.africa/2024/09/19/nigerias-digital-transformation-and-ai-ready-data-centres-rack-centre-leading-the-charge/> accessed 15 September 2024.

(NDPR) of 2019 introduced some provisions for data localization, but it remains to be seen how these will be implemented and enforced.[11]

This paper aims to examine the impact of data localization on international trade obligations in the context of Nigeria's digital economy. By analysing the potential conflicts and exploring policy options for balancing data sovereignty with trade facilitation, this research intends to contribute to the ongoing discourse on data governance and economic development.

1.1 The Digital Economy in Nigeria: An Overview

The digital economy, also known as the 'internet economy', 'new economy' or 'web economy', is a driving force in the global economic landscape.[12] In 2016, the digital economy accounted for 15.5% of the world's overall gross domestic product (GDP), amounting to USD11.5 trillion.[13] While developed nations like the United States, the United Kingdom, Germany and Japan have long been at the forefront of digital advancements, developing countries, including Nigeria, have increasingly recognised the need to integrate digital technology into their economic restructuring.[14]

The Nigerian government has taken steps to foster the country's digital economy. This includes renaming the Federal Ministry of Communications to the Federal Ministry of Communications and Digital Economy, as well as introducing economic policies and investments aimed at developing the necessary information and communications technology (ICT) capacity and infrastructure.[15] Nigeria's Economic Recovery and Growth Plan 2017–2020 and the National Digital Economy Policy and Strategy 2020-2030 have further underscored the government's commitment to harnessing the benefits of a digital economy.[16]

Despite these efforts, Nigeria's digital economy remains largely underdeveloped. Challenges such as low broadband penetration, insufficient ICT infrastructure, and a lack of technological readiness continue to hinder the country's digital transformation.[17] One significant issue that has emerged in this context is the question of data localisation, which will be the focus of the subsequent sections.

2.0 Navigating Data Sovereignty and Regional Trade: Nigeria's Approach to Data Localisation

2.1 Data Localisation and Data Protection in Nigeria

The unrestricted movement of data is a key enabler of the digital economy. However, the development of data protection and data localisation policies has become a significant area of concern for

[11] Nigeria Data Protection Act (NPDA) 2023; Nigeria Data Protection Regulation (NDPR) 2019.
[12] Jacek Unold, *Basic Aspects of the Digital Economy* (Acta Universitatis Lodziensis 2003) 41.
[13] HA Zubairu and others, 'Assessing the E-readiness of Nigeria for Digital Economy' [2020] (8)(2) *American Journal of Computer Science and Information Technology* 50.
[14] *Ibid.*
[15] Federal Ministry of Communications and Digital Economy, 'National Digital Economy Policy and Strategy (2020-2030),' https://www.ncc.gov.ng/docman-main/industry-statistics/policies-reports/883-national-digital-economy-policy-and-strategy/file.
[16] (n. 6).
[17] Zubairu (n 13).

international trade and investment.[18] This is particularly true for e-commerce and internet-based services, which heavily rely on cross-border data flows.[19] While the free flow of data across borders brings economic benefits, it also raises concerns about security, surveillance, law enforcement, and the potential violation of individuals' right to privacy and personal data protection.[20] In response, countries have established data privacy regimes to mitigate the risks associated with transborder data flows.

As part of these efforts, a growing number of emerging economies, including Nigeria, have introduced data localisation measures. Data localisation refers to requirements that restrict the transfer of data across national borders.[21] These measures range from strict prohibitions on data exports to more lenient approaches, such as requiring copies of data to be stored domestically or imposing taxes on data exports.[22]

Nigeria is recognised as one of the emerging economies with a relatively strict approach to data localisation. Recently, the Government of Nigeria enacted the Nigerian Data Protection Act (NDPA) 2023, a dedicated data privacy law.[23] Prior to the introduction of the NDPA 2023, the right to privacy was guaranteed by the Constitution of the Federal Republic of Nigeria 1999, while in 2019, the National Information Technology Development Agency (NITDA) introduced the Nigeria Data Protection Regulation (NDPR) 2019 to ensure data privacy and enable Nigerian companies to remain competitive in international trade.[24] Beyond the NDPR, NITDA has also implemented various other legal instruments to promote data localisation in the country. The agency recently published its privacy policy to guarantee the privacy rights of all persons whose personal information is stored in its database. The policy also addresses the 'clear negative trade balance' in the information technology (IT) sector by setting a target of 50% local content threshold for goods and services in the IT sector. To further this objective, NITDA introduced several measures purportedly to encourage indigenous innovation.[25]

In 2019, NITDA introduced another initiative with a data-localisation effect with the release of the National Cloud Computing Policy issued pursuant to Section 6 (a–c) of the NITDA Act.[26] The policy aims to promote the adoption of cloud computing by the Nigerian government and small and medium-sized enterprises (SMEs). The policy regards 'government data' as 'data produced or commissioned by government or government-controlled entities'.[27] This invariably covers a large collection of data and databases. While the policy encourages cross-border data flow, it requires that 'agencies must do so in line with the requirements of the Nigerian Data Protection Regulation and any other content

[18] GSMA, 'The Impact of Data Localisation Requirements on the Growth of Mobile Money-Enabled Remittances,' <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/03/GSMA_Understanding-the-impact-of-data-localisation.pdf> accessed 16 September 2024.
[19] *Ibid*.
[20] Anupam Chander and Uyen P Le, 'Data Nationalism' [2015] (64)(3) *Emory Law Journal* 680.
[21] *Ibid.*
[22] *Ibid*.
[23] National Data Protection Act (NDPA) 2023.
[24] Constitution of the Federal Republic of Nigeria 1999; Nigeria Data Protection Regulation (NDPR) 2019.
[25] NITDA, 'https://nitda.gov.ng/wp-content/uploads/2020/11/NCCPolicy_New1.pdf' <https://nitda.gov.ng/wp-content/uploads/2020/11/NCCPolicy_New1.pdf> accessed 28 November 2024.
[26] NITDA, 'Nigeria Cloud Computing Policy'.
[27] *Ibid* 5.

regulation'.[28] Thus, federal public institutions are only to contract cloud service providers that will store data in a jurisdiction that provides a level of data protection similar to Nigeria.[29]

2.2 The Role of Nigeria Data Protection Commission (NDPC)

The Nigeria Data Protection Commission (NDPC), established in 2022, is responsible for enhancing data privacy protection in Nigeria. Its measures on data localisation aim to strike a balance between safeguarding citizens' privacy and fostering economic competitiveness. The commission is empowered by section 4 to 8 of the Nigeria Data Protection Act (NPDA) 2023 to administer and enforce laws and regulations that will enhance data localisation and the enhance digital economy of the nation.[30]

2.3 Role of the Nigeria Communication Commission

The Nigerian Communications Commission (NCC) also contributes to data localisation with the NCC's Telephone Subscribers Regulations 2011.[31] This regulation provides for the privacy and protection of personal data of telephone subscribers in Regulations 9 and [32]Specifically, the regulation imposes obligations on the licensees to ensure that the personal information of subscribers is stored in confidence. This information is not to be released to third parties nor to be transferred outside of Nigeria without first obtaining the consent of the subscriber and of the NCC. All information stored in the central database is regarded as the property of the federal government of Nigeria.[33]

2.4The Role of the Central Bank of Nigeria (CBN)

The Central Bank of Nigeria (CBN), in exercising its powers under Section 47(3) of the Central Bank of Nigeria Act, 2007, issued the Guidelines on Point of Sale (POS) Card Acceptance Services (POS Guidelines), which regulates all domestic transactions performed with payment cards.[34] Specifically, Regulation 4.4.8 provides that: All domestic transactions including but not limited to POS and ATM transactions in Nigeria must be switched using the services of a local switch and shall not under any circumstance be routed outside Nigeria for switching between Nigerian Issuers and Acquirers.[35]The implication of the above is to ensure the protection of data accessed by POS and ATM handlers.[36]

3.0 Data Localisation, International and Regional Trade Law, and Nigeria's Obligations

The Nigerian economy is acknowledged to be the largest in Africa and the 26th largest in the world, and as such, any policy that affects trade would not only impact the country but may also affect its

[28] *Ibid.*
[29]Emma Okonji, 'Experts Highlight Benefits of Data Localisation, Cloud Adoption in Nigeria', This Day, November 7, 2019.
[30] Nigeria Data Protection Act (NDPA) 2023, ss 4-8.
[31] Nigerian Communications Commission (NCC), 'Registrations of Telephone Subscribers' Regulations 2011', https://www.ncc.gov.ng/docman-main/legal-regulatory/regulations/201-regulations-on-the-registration-of-telecoms-subscribers/file.
[32] *Ibid.*
[33] *Ibid.*
[34] Central Bank of Nigeria (CBN), 'Guidelines on Point of Sale (POS) Card Acceptance Services', https://www.cbn.gov.ng/cashless/POS_GUIDELINES_August2011_FINAL_FINAL%20(2).pdf.
[35] *Ibid.*
[36] *Ibid.*

relationship with Africa and the world at large.[37] Over the years, Nigeria has tried to use trade, including international and regional trade, to stimulate its economic potential.[38].

Some of these trade instruments will be examined.

3.1 African Continental Free Trade Area (AfCFTA)

Pursuant to the Lagos Plan of Action, 1980,[39] the African Union (AU) began the creation of the African Economic Community through a free trade area, customs union, and a common market amongst the 55 African Member States.[40] To achieve greater cohesion and economic integration within the continent, the AfCFTA Agreement was created. The Agreement seeks to make intra-African trade easier and more competitive through the minimisation of tariff and non-tariff barriers and the gradual elimination of 90% tariffs within five to fifteen years.[41]

Nigeria signed the AfCFTA Agreement in July 2019 and ratified it on 5 December 2020.[42] The Agreement is aimed at increasing intra-African trade by creating a liberalised market and delivering a wide-ranging and constructive trade agreement among the Member States.[43] The main objectives of AfCFTA are to: create a single continental market for goods and services, with free movement of business persons and investments; expand intra-Africa trade across the regional economic communities and the continent in general; and enhance competitiveness and support economic transformation.[44] AfCFTA has eased the flow of services and information among member countries, and its resultant effect is that there is an obligation on each Member State to ensure the free flow of data, including personal data of their citizens, to other member countries. This is especially necessary for digital trade and e-commerce. Inevitably, this creates a sharp contrast between the objectives of AfCFTA and Nigeria's data localisation policies. Thus, the data protection frameworks in Nigeria need to be compatible with the international trade regime if the country is to benefit from the global digital economy under the several bilateral and multilateral trade agreements to which it is a party.[45]

[37]John Onyido, Ibidolapo Bolu and Oluwasolape Owoyemi, 'Nigeria: Developments in Investment and Intraregional Trade in Africa', https://www.mondaq.com/nigeria/international-trade-investment/727066/developments-in-investment-and-intraregionaltrade-in-africa?login=true.
[38] *Ibid*.
[39] See the Treaty Establishing the African Economic Community, Lagos Plan of Action for the Economic Development of Africa 1980–2000 4 (1980); Adopted on 3 June 1991; entered into force on 12 May 1994.
[40] See the Preamble and Art. 3 of the 'Agreement establishing the African Continental Free Trade Area (AfCFTA)'.
[41] African Union, Report to the Specialized Technical Committee on Trade, Industry and Minerals: Progress on the African Continental Free Trade Area (AfCFTA) for the Period from May 2016 to Dec. 2018, 2& 3 (AUC/DTI/AfCFTA/STC/Rep/D). See further Oyeniyi Abe and Sewagegnehu Taye, 'The 'Flexibility' Standard in the African Union and Its Ramification for the Implementation of the African Continental Free Trade Area (AfCFTA) Agreement', Global Trade and Customs Journal 16, no. 2 (2021): 80.
[42] 'Status of AfCFTA Ratification', https://www.tralac.org/resources/infographic/13795-status-of-afcfta-ratification.html.
[43] See the Agreement Establishing the African Continental Free Trade Area https://au.int/sites/default/files/treaties/36437-treatyconsolidated_text_on_cfta_-_en.pdf.
[44] Tralac, 'The African Continental Free Trade Area: A Tralac Guide', https://www.tralac.org/documents/resources/booklets/4062- afcfta-a-tralac-guide-7th-edition-august-2020/file.html.
[45] Tralac, 'Data Protection Regulations and International Data Flows: Implications for Trade and Development', April, 19, 2016 https://www.tralac.org/news/article/9500-data-protection-regulations-and-international-data-flows-implications-for-tradeand-development.html.

AfCFTA provides a significant avenue for Nigeria to enhance its trade relations with other African states. However, implementation remains a challenge. On the one hand, lowering tariffs could help diffuse trade challenges, while on the other, restructuring non-tariff and trade facilitation measures may cause significant policy reforms at the national level. To remain competitive and to confront Africa's economic fragmentation, trade barriers must be eliminated.[46] However, significant barriers – such as non-tariff barriers in services, fragmented rules designed to promote investment, and data localisation policies – impede trade facilitation.[47] Protectionist policies such as data localisation can be maintained in sectors that do not contribute significantly to the economy. Deepening regional integration calls for heightened scrutiny on cross-border trade, which goes undetected.[48] The eradication or non-deference to data localisation will foster economic transactions and reduce the 'prices of imported goods for consumers and producers using intermediate inputs'.[49] Since not all countries have data localisation policies within the continent, Nigeria's data localisation policies will undoubtedly create an onerous administrative process, thereby stifling trade. This means that data protection as a policy objective must be adapted in trade rules governing data transfers.[50] The application of different rules and domestic regulations may frustrate the aims of AfCFTA, thereby leading to compliance and operational costs.[51]

Within the rubric of trade facilitation guaranteed under WTO rules, AfCFTA becomes instructive. However, the invention and implementation of AfCFTA could become a mirage where protectionist measures conflate with free trade obligations. In the next section, we will discuss Nigeria's trade obligations under various bilateral agreements and the multilateral trading system of the WTO. We consider the importance of a steady, malleable, and harmonious data localisation measure that could facilitate trade. Otherwise, protectionist measures that hamper trade commitments could severely affect Nigeria's standing in the international trade community.

3.2 AfCFTA Rules and Data Localisation

Nigeria's data localisation measures appear to align with local content requirements for employment generation and local investment. However, such policies could end up being counterproductive, as they may hinder international investment and trade facilitation. The phenomenon of regional trade agreements (RTAs) encourages cooperation between members of a trade arrangement. The WTO guarantees an effortless, predictable, and free flow of trade if there is no detrimental effect.[52] To ensure this, any form of obstacle must be removed. One such obstacle is data localisation by Member States. Granted that trade relations sometimes involve conflicting interests between investors, stakeholders, and states, the actualisation of data localisation creates an extreme barrier to trade. Consequently, it appears as if AfCFTA does not regulate data localisation procedures. Rather, it provides some model

[46] Neha Mishra, 'Data Localisation Laws in a Digital World', Public Sphere, 2016 Issue, (2016):137
[47] Maryla Maliszewska et al., The African Continental Free Trade Area: Economic and Distributional Effects (Washington: The World Bank, 2020).
[48] *Ibid.*
[49] *Ibid.*
[50] Susannah Hodson, 'Applying WTO and FTA Disciplines to Data Localisation Measures', World Trade Review 18, no.4 (2019): 581.
[51] See further Maryla Maliszewska et al., The African Continental Free Trade Area, 41.
[52] Oyeniyi Abe, 'Deepening Regional Integration and Organizing World Trade: The Limits of ECOWAS', International Journal of Public Law and Policy 4, no.1 (2014): 72.

of protection alongside actions, which constrains the 'cross-border transfer and storage of data',[53] particularly where such restrictions are aimed at international investors. Furthermore, AfCFTA does not seem to address the challenges imposed by such requirements that attempt to disregard national treatment and market access commitments for foreign investors. At the WTO level, there has been no dispute or challenge to data localisation measures. Hence, the extent to which Nigeria's data localisation requirements are allowed under WTO rules or whether they impede trade remains unclear.

Notably, the General Agreement on Trade in Services (GATS), 1995, allows Member States to 'regulate the supply of services in pursuit of their own policy objectives'.[54] Services are not defined under the Agreement. However, Article 1.2 (a) defines 'trade in services' to include the supply of services from one country to another. Nigeria's commitment to GATS does not limit the provision of any services, except to show that all foreign commercial activities must be domesticated in Nigeria.[55] The application of the principle of technological neutrality in Nigeria, whereby data localisation requirements prevent access to the online delivery of services, could be a breach of Nigeria's commitment under treaty frameworks. As a result, where not sensitively applied, data localisation measures could breach Nigeria's market access and national treatment commitments under AfCFTA.

Nigeria is yet to make a full commitment under AfCFTA. It is therefore difficult to conclude whether it can impose a market access barrier impeding foreign investors from operating in the domestic market. If Nigeria has made full commitments under AfCFTA, it cannot claim or require foreign investors to be domesticated before they can operate locally,[56] or restrict cross-border data transfers, especially through electronic means. For example, Nigeria could require international telecommunications traffic to be routed through a domestic carrier, instead of the preferred international carrier. This act could be in violation of Nigeria's commitment under regional and international treaties as it attempts to impose a zero quota on the cross-border supply of services. Besides, Article XVII of GATS prohibits any form of discrimination against foreign suppliers in sectors that Member States have committed to – including the telecommunication and financial sectors of Nigeria.

Data localisation measures that prevent the actualisation of the most favoured nation clause under WTO rules deserve some level of heightened scrutiny, especially regarding the 'effect and trade impact of the measure'.[57] A broadly couched data localisation protectionism measure will most certainly violate trade obligations and commitments under treaty regimes.[58] The exceptions to these trade rules allow Member States to deviate from market access and national treatment commitments.[59] These exceptions are anchored on public morals and protecting the right to privacy, which may allow Nigeria to craft policies that could limit cross-border data transfers in the interests of policy measures. Hence, data protection

[53] Susannah Hodson, 'Applying WTO and FTA Disciplines to Data Localisation Measures', World Trade Review 18, no.4 (2019): 583.
[54] Article XIX of the General Agreement on Trade in Services (GATS) https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm.
[55'] Nigeria, Schedule of Commitment's', https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=Q:/SCHD/GATS-SC/SC65. pdf&Open=True..
[56] See further Article XVI, paragraph 2 of GATS.
[57] Hodson, 'Applying WTO and FTA Disciplines', 592.
[58] See Article XIV (a) (c) (ii) of GATS.
[59] Article XIV (a) (c) (ii) of GATS.

laws that prevent data harvesting or the storage of data outside Nigeria to protect individual privacy, could fall under GATS exceptions. Consequently, Nigeria's commitments under its trade treaties could be jeopardised where data localisation measures limit the exercise of those commitments. However, this is inconclusive as there are no final decisions from the Appellate Body ruling with finality on the conflict between data localisation and commitments to free trade under bilateral agreements. Unfortunately, the absence of judicial examination 'considering data localisation measures means significant legal uncertainty remains about how such measures would be treated under the GATS'.[60]

3.2 AfCFTA Regulations on Cross-Border Data Flow

Articles 6 and 15 (c) (ii) of AfCFTA's Protocol on Trade in Services regulate the ability of Member States to transfer and store data across national borders. While Article 6 prevents Nigeria from disclosing confidential information and data where such disclosure will impede law enforcement or be contrary to the public interest – 'prejudice legitimate commercial interests' of businesses[61] – the general exemption from the AfCFTA data provisions under Article 15 (c) (ii) allows Nigeria to adopt protectionist measures, such as data localisation, where such measures guarantee 'the protection of the privacy of individuals in relation to the processing and dissemination of personal data and protecting confidentiality of individual records and accounts'.[62]

While AfCFTA does not have a protocol on cross-border data transfer, we believe that data localisation without adequate rationale disrupts the true intention of AfCFTA. In effect, Article 6 facilitates cross-border data flow by permitting businesses to transfer data among Member States. However, where the transfer of data concerns any of the identified factors, such factors will be prohibited. For example, if a Nigerian telecommunications service supplier seeks to transfer data relating to its operations in South Africa to the suppliers' headquarters in Lagos, it may do so unless such transfer will obstruct law enforcement, will be contrary to public interests, and will prejudice legitimate commercial interests of other businesses. Furthermore, data localisation guaranteed under Article 15 (c) will only be justified where the reasons for such restrictions are not enforced in a way that will constitute 'arbitrary and unjustifiable discrimination' between Member States.[63]

A combined effect of these rules does not prevent State Parties from adopting trade restrictions in pursuit of legitimate commercial interest, provided such interests are not 'arbitrary and unjustifiable'. The horizontal effect of these provisions enables State Parties to craft a broad scope of policy objectives to protect their citizens. The question is how legitimate data localisation measures are in Nigeria to warrant consideration of policy objective determination. AfCFTA provides no guidance, and it is expected that any reason or policy goals on security, health, or education would suffice.

Article 15 (c) (ii) of AfCFTA retroflex the requirement under Article XIV (c) (ii) of GATS which provides that measures should not be applied arbitrarily. In effect, the AfCFTA data rules appear to be more expansive than the GATS approach as it includes data localisation measures that do not constitute

[60] Hodson, 'Applying WTO and FTA Disciplines', 596.
[61] See Article 6 of AfCFTA's Protocol on Trade in Services.
[62] Article 15 (c) (ii) of AfCFTA's Protocol on Trade in Services.
[63] Article 15 (c) (ii) of AfCFTA's Protocol on Trade in Services.

'breach of national treatment or market access' obligations of the WTO.[64] Thus, under the AfCFTA rules, Nigeria could require local and international investors to store data on servers within either Nigeria or a State Party's jurisdiction before commencing business. Such an action will not violate national treatment or market access as those acts are non-discriminatory.

The implication of these provisions is that multilateral and trade obligations protect data localisation measures where data is stored within the borders of Nigeria, despite the restriction of transferring data across borders. Both articles read jointly preserve the sovereignty of Member States to enact laws that restrict the flow of data subject to some exemptions. It is not yet clear how these provisions will be interpreted practically or before a dispute settlement body, given the new and innovative Agreement. However, for proper context, these articles must be read with the general objectives under Article 3 of the Protocol, which enhances the intentions of AfCFTA. The AfCFTA Agreement broadly seeks to achieve 'an integrated, prosperous and peaceful Africa' by creating a single and liberalised market for goods and services.[65] While AfCFTA does not have a protocol on cross-border data transfer, we believe that data localisation without adequate rationale disrupts the true intention of AfCFTA, despite the exception the Agreement grants in order to be involved in trade activities.

The AfCFTA provisions allow parties to preserve measures that appear to be inconsistent with the AU data protection regime. For instance, Article 14 (6) (a) of the African Union Convention on Cyber Security and Personal Data Protection (discussed below) prohibits data transfer to Non-member States except if 'the state ensures an adequate level of protection of the privacy, freedom, and fundamental rights of persons whose data are being or are likely to be processed'.[66] While we concede that inadequate data protection can negatively affect market access and productivity, we are of the view that exceedingly rigid protection can constrain business activities with attendant unfavourable economic effects.

While AfCFTA contains some provisions on data protection and the conduct of trade, the remaining challenge is the dispute between provisions of regional instruments that impedes multilateralism guaranteed under WTO principles, which could have the capability of global trade distortion.

4.0 African Union Convention on Cyber Security and Personal Data Protection (The Malabo Convention)

The Malabo Convention is another instrument that creates trade obligations for Nigeria. Indeed, issues of cybercrime and cybersecurity have become worrisome in Africa. Specifically, cybercrime and cybersecurity could also be a trade barrier because it creates a lack of trust in an e-commerce platform. This fact is recognised even in the Convention's preamble where it is stated that 'the major obstacles to the development of electronic commerce in Africa are linked to security issues'.[67] The Malabo Convention therefore encourages AU Member States to recognise the need to protect personal data and to encourage the free flow of information to develop a credible digital space in Africa. Since the

[64] Susannah Hodson, 'Applying WTO and FTA Disciplines to Data Localisation Measures', World Trade Review 18, no.4 (2019):605.
[65] See Article 3 of AfCFTA Agreement. See also Article 3 (2) (e) of AfCFTA's Protocol on Trade in Services.
[66] Close variant to this is in Article 36 of ECOWAS Supplementary Act A/SA.1.01.10 on Personal Data Protection Within ECOWAS https://www.statewatch.org/media/documents/news/2013/mar/ecowas-dp-act.pdf.
[67] See the Preamble to the AU Convention.

adoption of the Convention, only 30 out of 55 African nations have passed or drafted privacy laws and only 13 of them have data protection authorities.[68] This convention is brought about by the increase in international trade, international relations and cybercrime, which are all direct results of advancement in ICT.

Article 11 of this Convention encourages Member States to establish independent bodies to protect personal data, whereas Article 12 encourages Member States to establish limits on the processing and storage of data, with exception to public interest. The Convention significantly grants Member States the right to discontinue the processing of data, block some aspects of collected data and either temporarily or permanently prohibit data processing in emergency situations that affect fundamental rights and freedom.[69] A good example would be the collection of an individual's data for a lawful purpose and using such data for an unlawful purpose.

The Convention acknowledges the need to obey national constitutions and international law. In the Convention preamble, it also states that the establishment of a regulatory framework on cybersecurity and personal data protection should consider the need to respect the rights of citizens, which is guaranteed under the fundamental texts of domestic law and protected by international human rights conventions and treaties, particularly the African Charter on Human and Peoples' Rights. Importantly, the Convention urges Member States to establish legal and institutional frameworks for data protection and cybersecurity, which they could achieve by either establishing new institutions or use existing ones.

The Convention also outlines the principles that ought to be adhered to in processing personal data, such as consent and legitimacy; lawfulness and fairness; purpose, relevance, and storage of processed personal data; accuracy; transparency, confidentiality and security of personal data. It further enjoins state parties to prohibit any data collection and processing without consent that reveals racial, ethnic and regional origin, parental affiliation, political opinions, religious or philosophical beliefs, trade union membership, sex life and genetic information or data on the state of health of the data subject, except under certain exceptional circumstances.[70]

There are expectations that trade commitments must be adhered to. Furthermore, the creation of big data and data sharing frameworks without supervisory mechanisms could lead to state [71]surveillance and violation of citizens' right to privacy, which contradicts the intent of data localisation measures.

4.1 ECOWAS Protocol on Free Movement of Persons, Goods and Services

ECOWAS is a regional group consisting of 15 members. Founded on 28 May 1975 through the Lagos Treaty, it was designed to encourage economic integration across the region. Considered one of the pillars of the African Economic Community,[72] ECOWAS was also designed as a single large trading

[68] Abdi Latif Dahir, 'Africa isn't Ready to Protect its Citizens Personal Data Even as EU Champions Digital Privacy,' Quartz Africa, May 7, 2018, https://qz.com/africa/1271756/africa-isnt-ready-to-protect-its-citizens-personal-data-even-as-eu-champions-digitalprivacy/.
[69] Kaitlin M Ball, 'Introductory Note to African Union Convention on Cyber Security and Personal Data Protection', International Legal Materials 56, (2017):164
[70] Lukman Adebisi Abdulrauf and Charles Manga Fombad, 'The African Union's Data Protection Convention 2014: A Possible Cause for Celebration of Human Rights in Africa?,' Journal of Media Law 8, no. 1(2016): 67.
[71] Economic Community of West African States 'Basic Information', https://www.ecowas.int/about-ecowas/basic-information/
[72] Article 1 of the Economic Community of West African States (ECOWAS) Revised Treaty, https://www.ecowas.int/wp-content/ uploads/2015/01/Revised-treaty.pdf.

bloc 'through an economic and trading union'.[73] The Revised Treaty establishes a common market through trade liberalisation.

The fundamental objective of the organisation is to facilitate cooperation and development in economic activity, and various sectors of the economy, to contribute to the progress and development of the African continent.[74] It is against this backdrop that the ECOWAS Protocol Relating to Free Movement of Persons, Residence and Establishment was drafted on 29 May 1979 to facilitate the achievement of the set objectives of the regional organisation.[75] Consequently, the first phase of the protocol – the protocol on free movement of persons, goods and services was ratified in 1980 and national committees were set up in Member States to monitor and ensure the implementation of the protocol.[76] Understandably, data localisation measures will be in direct contrast with the right of citizens of ECOWAS Member States to establish businesses.

The ECOWAS Protocol on the Free Movement of People and Goods ensures free mobility of the community citizens. It allows citizens of Member States the right to enter and reside in the territory of another Member State, provided they possess a valid travel document and an international health certificate. However, it also allows Member States the right to refuse admission to any community – citizens who were inadmissible under the Member State's own domestic law.[77] While seeking to create a regional market for citizens of Member States, the goals speed up the socio-economic development of the region.

The Protocol does not define what constitutes goods or services, neither does it provide for cross-border data transfer. The only prohibition relates to persons who are inadmissible under the Member State's own domestic law. In facilitating economic activity within the sub-region, it appears as if this Protocol overrides any data protectionist measures of Member States to the extent that those measures prohibit the right to establish or restrict the free movement of services that encompass data.

4.2 ECOWAS Supplementary Act on Data Protection (2010)

ECOWAS is mindful of the need to promote regional trade among Member States and has recognised the fact that issues of data protection could be an obstacle to this goal. It is in light of this that the ECOWAS Supplementary Act on Data Protection was adopted.[78] The Supplementary Act directly applies in Member States, and creates an obligation on members to 'establish a legal framework of protection for privacy of data relating to the collection, processing, transmission, storage, and use of personal data without prejudice to the general interest of the State'.[79] While there is currently limited activity surrounding the implementation or actualisation of the Act, it remains a formidable instrument

[73] Olayiwola Ojo Abe, 'Deepening Regional Integration in West Africa: A Comparative Analysis of the ECOWAS and the EU', NU International Journal of Public Administration 39, no. 2 (2016): 74.
[74] ECOWAS Treaty, 1975; Article 2.
[75] ECOWAS Protocol on Free Movement of Persons and the Right of Residence and Establishment A/P.1//5/79.
[76] *Ibid.*
[77] Abimbola Opanike and Ayodeji Anthony Aduloju 'ECOWAS Protocol on Free Movement and Trans-border Security in West Africa', Journal of Civil and Legal Sciences 4, no. 3 (2015):154.
[78] ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection, Article 2.
[79] (n. 78).

that seeks to balance the data privacy rights of citizens of Member States with the trade liberalisation objectives of the community.

4.3 West Africa–European Union Economic Partnership Agreement

The main aim of the West Africa–European Union Economic Partnership Agreement (EPA) is the establishment of a free trade area between Europe and West Africa in accordance with Article XXIV of the General Agreement on Tariffs and Trade (GATT), through the gradual removal of trade restrictions between the two trade partners.[80] The EPA is intended to foster the smooth and gradual integration of African, Caribbean and Pacific (ACP) states into the world economy, with due regard for their political choices and development priorities, thereby promoting their sustainable development and contribution to poverty eradication. EPA negotiations were officially launched at an all-ACP level on 27 September 2002.[81]

EPAs are legally binding bilateral contracts between the European Union (EU) and individual African countries. EPAs represent a fundamental shift in the trading relationships between the two parties, from a non-reciprocal preferential trading regime under which 'ACP' countries could export almost freely to the EU while maintaining their own restrictions on EU imports, to one requiring reciprocity in liberalisation, albeit with a certain degree of asymmetry in commitments, in line with rules of the WTO.[82] This, however, has been criticised as a 'pyrrhic victory' since prematurely opening markets can make African agricultural and non-agricultural production find it very difficult to compete with the likely cheaper, perhaps better quality and even larger supply of goods and services from European countries.[83]

The EPA includes several safeguards that can be implemented if liberalised products are increasing too rapidly, thus endangering local markets.[84] Data protection or localisation is not one of those safeguards. However, considering that the EPA is between the EU and West Africa as a bloc, no Member State will be allowed to evade its obligations under the Agreement as a result of domestic policies that do not relate to agricultural products.[85] The EPA strongly advances West Africa's integration into the global trading system while supporting investment and economic development of the region.[86]

5.0 The Effect of Nigeria's Data Localisation Policies on its Trade Liberalisation Obligations

The countless opportunities that digital technology offers can be leveraged by developing countries, like Nigeria, to diversify their economy.[87] These opportunities can be effectively harnessed with the unrestricted flow of both personal and non-personal data. The trade agreements to which Nigeria is a party create one overarching obligation – to ensure cross-border trade with no form of hindrance,

[80] ECOWAS, 'Economic Partnership Agreement', https://www.ecowas.int/doing-business-in-ecowas/epa/.
[81] *Ibid.*
[82] Kelechi C. Nnamdi and Kingsley C Iheakaram, 'Impact of Economic Partnership Agreements (EPA) on African Economy: A Legal Perspective', http://cega.berkeley.edu/assets/miscellaneous_files/6-ABCA-Nnamdi-Impact_of_EPA_on_AFR_economy.pdf.
[83] Nnamdi and Iheakaram, 'Impact of Economic Partnership Agreements'.
[84] European Commission, 'West Africa'.
[85] (n 84).
[86] *Ibid.*
[87] Particularly because data collection and storage is an integral part of digital technology and because data is now regarded as the new oil.

especially at the regional level, while also protecting privacy (and other sovereign values).[88] The implication of this huge obligation is that laws and policies put in place by the country must align with its free trade obligations, including data localisation policies.

While data localisation measures significantly affect trade, especially in the information society, it also has many policy justifications.[89] Indeed, according to John Selby, 'proponents of data localisation laws have typically raised some or all of the following four arguments as justification for their recommendations: data localisation provides better information security against foreign intelligence agencies; data localisation supports the local technology industry; data localisation protects the privacy and security of citizens' data; and data localisation supports local law enforcement'.[90] In essence, the overall effect of the NCDC, NITDA, NCC and CBN regulations and policies, which promote the localisation of data, are mainly justified on the grounds of privacy and the support of the local information technology industry.[91] These localisation policies also have the effect of protecting Nigeria's digital sovereignty.[92]

The efforts made at the domestic level to develop Nigeria's digital economy must be matched with a sustained commitment to its regional obligations.[93] As mentioned, no nation can effectively develop today without paying close attention to the goldmine lying underneath the digital space. Nigeria's increasing move toward greater localisation of data with its many policies therefore has an impact on its commitment under international and regional treaty law – especially in the following crucial ways.

First, data localisation is a key barrier to digital trade. Indeed, traditional services can now be transacted across borders through digital means. However, data is the hallmark of any digital transaction and where there are restrictions to the availability of data, this would throw a spanner in the works of digital trade.[94] Consequently, Nigeria's obligation to guarantee free trade under relevant treaties could be affected by its strict data localisation measures.[95] In this regard, the United State National Association of Manufacturers puts it succinctly that: 'such trade barriers… take forms of not only traditional trade and investment restrictions, but also forced localisation barriers that pressure companies to move manufacturing and operations overseas, intellectual property theft that undercuts manufacturing competitiveness, problematic import and export policies that distort global trade and discriminatory technical barriers to trade that block imports and create advantages for domestic producers'.[96]

[88] Kelechi C. Nnamdi and Kingsley C Iheakaram, 'Impact of Economic Partnership Agreements (EPA) on African Economy: A Legal Perspective', http://cega.berkeley.edu/assets/miscellaneous_files/6-ABCA-Nnamdi-Impact_of_EPA_on_AFR_economy.pdf.
[89] John Selby, 'Data Localisation Laws: Trade Barriers or Legitimate Responses to Cyber-security Risks, or both? International Journal of Law and Information Technology 25, no. 3 (2017): 213.
[90] (n. 89).
[91] Olajumoke Kukoyi and Taiwo Oriowo, 'Data Protection and Privacy Laws in Nigeria', https://www.mondaq.com/nigeria/data-protection/1071394/data-protection-and-privacy-laws-in-nigeria.
[92] *Ibid.*
[93] ECOWAS, 'Economic Partnership Agreement', https://www.ecowas.int/doing-business-in-ecowas/epa/.
[94] J Ferencz and F Gonzales, 'Barriers to Trade in Digitally Enabled Services in the G20', OECD Trade Policy Papers, no. 232, https:// www.oecd-ilibrary.org/trade/barriers-to-trade-in-digitally-enabled-services-in-the-g20_264c4c02-en.
[95] Hoagland Isabelle, 'Business, Tech Groups Flag Data Localisation Policies as Barriers to U.S', Inside US Trade 36, no. 45 (2018) https://www.proquest.com/docview/2131157486/fulltext/76D7F648B1B04C96PQ/1?accountid=11526.
[96] *Ibid.*

Second, Nigeria's data localisation drive leads to an increase in operational cost for global multinational companies with a potential back-end effect on consumers.[97] Most trade agreements entered by Nigeria guarantee free trade at the best possible prices and stabilise export prices and commodity supply.[98] However, it is an established fact that data localisation will require that data is saved within a particular country.[99] This means there is a duty imposed on the government to ensure an effective system and this would lead to higher operational costs for the country. Thus, to fulfil its free cross-border trade obligations, Nigeria will be required to store data at two places, and this would shoot up operational costs resulting in extra financial burden on the government, which is then passed on to consumers.[100]

Third, data localisation leads to unhindered access of the government to personal data of individuals which are held by businesses. This points to data localisation as a potential tool for political repression: strict data localisation laws can enable a breach of privacy and data protection, anti-discrimination and freedom of expression, and democratic values. Localisation of data can cause unnecessary regulation of citizens since the government can easily control and monitor the data of citizens.[101]

Consequently, the disadvantages of data localisation far outweigh its benefits.[102] Very few local entrepreneurs reap the benefits of data localisation, while the damage of data localisation is felt across all forms of businesses who will be prevented from accessing global services that could enhance their productivity.[103] The associated benefits of the multilateral trade regime and digitalisation can be disrupted by protectionist policies that inflict burdensome and exorbitant trade rules on businesses.[104] Indeed, Nigeria's reason for data localisation is anchored on the local economic development rationale.[105] However, evidence shows that data localisation has increased costs for local businesses, stifled innovation and technological inventiveness, and has impeded access to the global market by local entrepreneurs.

6.0 Conclusion

Nigeria's efforts to promote its digital economy must be aligned with its regional and international obligations. While data localization measures may provide some level of protection for personal data and national sovereignty, they can also hinder cross-border trade and economic growth. The country must find a balance between data sovereignty and trade facilitation to ensure the full benefits of the digital economy are realized. Nigeria can achieve this balance by adopting a data-driven approach to policymaking, conducting thorough impact assessments, and engaging in active dialogue with

[97] Diganth Raj Sehgal, 'Data Localization and Cross-border Data Transfers', https://blog.ipleaders.in/data-localization-cross-borderdata-transfers/.
[98] For instance, the International Commodity Agreements (ICAs).
[99] (n. 97).
[100] (n 97).
[101] Erica Fraser, 'Data Localisation and the Balkanisation of the Internet', SCRIPTed 13, no.3 (2016): 360-73.
[102] Jennifer Huddleston and Jacqueline Varas, 'Impact of Data Localisation Requirements on Commerce and Innovation', Insight June 16, 2020, https://www.americanactionforum.org/insight/impact-of-data-localisation-requirements-on-commerce-and-innovation/.
[103] *Ibid.*
[104] Theodore Claypoole, 'Data Localisation and the Limits of 'Everything from Everywhere' https://www.womblebonddickinson. com/us/insights/articles-and-briefings/data-localisation-and-limits-everything-everywhere.
[105] (n. 20) 677-739.

stakeholders locally, regionally, and internationally. Furthermore, Nigeria should continue to strengthen its cybersecurity infrastructure and promote digital literacy among its citizens. By taking these steps, Nigeria can harness the full potential of the digital economy while minimizing the risks associated with data localization.

7.0 Recommendation

Based on the findings of this research, the following policy recommendations are proposed to help Nigeria balance data sovereignty with trade facilitation in the digital economy:

The Nigerian government should collect and analyze data on the impact of data localization measures on trade, economic growth, and innovation. This data can be used to inform policy decisions and ensure that data localization measures are not overly burdensome or counterproductive.

Before implementing any data localization measures, the Nigerian government should conduct thorough impact assessments to identify the potential benefits and risks. These assessments should consider the impact on trade, economic growth, innovation, and human rights.

The Nigerian government should engage in active dialogue with stakeholders, including businesses, civil society organizations, and international partners, to discuss the potential impact of data localization measures. This dialogue should help to identify concerns and develop consensus on the best way to proceed.

Nigeria should continue to strengthen its cybersecurity infrastructure to protect personal data from unauthorized access and use. This includes investing in cybersecurity technologies, training cybersecurity professionals, and raising awareness of cybersecurity risks.

Nigeria should promote digital literacy among its citizens to help them understand the risks and benefits of data localization and to make informed decisions about how they share their personal data.

By implementing these policy recommendations, Nigeria can harness the full potential of the digital economy while minimizing the risks associated with data localization.