THE EMERGENCE OF A GLOBAL ECONOMY: THE DATA LOCALISATION PARADOX

By Victoria Oloni

ABSTRACT:

It is pertinent to adopt policies that encourage globalisation and transnational relations in the information age, not policies that restrict global trade. This article examines the concept of Data Localization, the objectives and implications of Data Localization. It examines the current legal framework for Data Localization in Nigeria, showing the long-term challenges it may pose to development. It also provides alternative policy measures that may be adopted in place of strict localisation laws. The article also examines data localisation policies from select countries in the world. This study employs secondary and qualitative research methods to arrive at its findings. From the research conducted, we found that mandatory data localisation creates several challenges, especially for developing economies like Nigeria, which include: negative economic impact, increased organisational cost, data vulnerability, an impediment to global trade and increased difficulties in the financial services sector. It is recommended that in place of data localisation, the Government should explore policy alternatives like conditional (soft) localisation, sectoral localisation or incentivising local storage of Data through tax incentives and improved infrastructure facilities.

1.0. INTRODUCTION

Over the last decade, over seventeen African countries have passed data localisation laws[1]. As of August 2019, more than 60 countries in the world have made regulations on Data Localization[2]. While addressing the First Annual Summit on Data Localization in Nigeria that held on 26 January 2016, the former Acting Director-General and current Director- eGovernment Development and Regulatory, NITDA, Dr Vincent Olatunji, stated that the Office for Nigerian Content Development role in achieving the Government's quest for the Localisation of Data hosting has become more critical now that data is the currency used among the internet community. He stated that:

> *"Why we are emphasising on Localisation of Data hosting are due to the huge benefits. If we are going to create jobs in the country, enable wealth creation, play better in the internet space*

[1] Lexi Novitske 'Data Localization Laws are Making African Trade Less Free' [20 September 2019] https://weetracker.com/2019/09/20/Data-Localization-laws-are-making-african-trade-less-free/ accessed on 20 June 2021

[2] Erik van der Marel , Matthias Bauer and Martina Ferracane, 'Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization' [2016], Global Commission on Internet Governance Paper Series. https://www.cigionline.org/publications/tracing-economic-impact-of-regulations-free-flow-of-Data-and-Data-Localization accessed on 20 June 2021

and ensure secured processes, especially now e-government, e-health, e-education, e-commerce, etc., are picking up, it is absolutely important that we follow the laws of the land."[3]

The above position appeared to reflect the Government's stance as regards data localisation, and this was reflected in the Data Protection Bill 2019. It was, therefore, a surprising but welcome development when the Data Protection Bill 2020 made a deviation from the localisation requirements in the 2019 bill and took a more liberal approach to localisation. This article examines the concept of Data Localization, the objectives and implications of Data Localization, alternatives to data Localisation, and the current legal framework for Data Localization in Nigeria.

1.1. Data Localisation

Data Localization has been defined as "the act of storing data on any device that is physically present within the borders of a specific country where the data was generated."[4] Chander and Lê broadly described it as a measure "that specifically encumbers the transfer of data across a national border."[5] Data Localisation can also be described as a policy that requires businesses to establish computing facilities within the host country's territory in which the business operates (localised Data hosting).[6] It could also be translated as an explicit requirement by a government for internet-based service providers to route data packets only within state borders (localised Data routing).[7]

1.2. Policy measures for Data Localization in Nigeria

1.2.1. The Data Protection Bill 2019 and the Draft Data Protection Bill 2020

The Draft Data Protection Bill 2020 abandons the Data Localization requirements of its predecessor, the Data Protection Bill 2019, which provided that Data Controllers and Data Processors of Personal

[3] Nigeria communication week ONC/NITDA, Rack Centre Ring Hope for Data Hosting in Nigeria, (27 January 2016) https://www.nigeriacommunicationsweek.com.ng/oncnitda-rack-centre-ring-hope-for-Data-hosting-in-nigeria-%E2%80%8E/?PageSpeed=noscript accessed on 20 June 2021

[4] What is Data Localization? - Definition from Techopedia. https://www.techopedia.com/definition/32506/data-localization accessed on 20 June 2021

[5] Anupam Chander and Uyên P. Lê, 'Data Nationalism' (2015) 64 Emory Law Journal 677, 678

[6] Kaushambi Bagchi and Sashank Kapilavai, 'Political Economy of Data Nationalism', (The 22nd Biennial Conference of the International Telecommunications Society: "Beyond the boundaries: Challenges for business, policy and society", Seoul, 24-27 June 2018) 4.

[7] John Selby, 'Data Localization laws: trade barriers or legitimate responses to cybersecurity risks or both?' (2017) 25 International Journal of Law and Information Technology; 213, 214

Data must record, systematise, accumulate, store, host, amend, update and retrieve Personal Data on devices that are physically located within Nigeria's territorial jurisdiction.[8]

The 2019 bill further provided in section 49 that a contravention of section 36 would lead to a fine of 8,000,000,000.00 (Eight Billion Naira) or not less than ten years imprisonment. The passage of this provision would have created difficulties for online content sharing and service providers who store personal Data belonging to Data subjects in Nigeria outside Nigeria.[9] The 2020 draft bill, however, provides that "Every data controller and data processor under this Act shall process personal data on devices under its control whether physically located within Nigeria or not"[10]. The only condition imposed by the Bill is that the data processor provides optimal technical and managerial measures to protect personal data against risks".[11]

1.2.2. National Cloud Computing Policy Version 1.2 August 2019

Although the Nigeria Cloud Computing Policy (NCCP) adopts a "Cloud First" proposition to Federal Public Institutions (FPIs) and SMEs, the policy also classifies data based on sensitivity, and this classification determines the Localisation policy be adopted. The policy classified Data in the following categories:

a. Official, public or non-confidential Data (Data of limited sensitivity):

This category is consists of data that is publicly available and non-sensitive. It is the most significant type of data held by public sector organisations. There is no requirement to store this kind of data locally.

b. Confidential, routine government business Data (Data of moderate sensitivity):

This category may include health and financial data about natural persons. This information can be securely held in a public cloud environment if appropriate safeguards are in place. This type of Data must reside primarily in a cloud framework within the Nigerian territorial boundary.

[8] Section 36 of the Data Protection Bill 2019
[9] Ibid.
[10] Section 33 of the Draft Data Protection Bill 2020 https://nationalpopulation.gov.ng/draft-data-protection-bill-2020/ accessed on 26 June 2021
[11] Section 34 of the Draft Bill available at https://nationalpopulation.gov.ng/draft-data-protection-bill-2020/ accessed on 26 June 2021

c. Secret, sensitive Government and citizen Data:

This type of data is related to natural and juridical persons. This data is classified as "sensitive" because the loss of confidentiality, integrity, or data availability could have serious, adverse, and material effects on the Data Subject or related entities. This type of Data must reside primarily in a cloud framework within the Nigerian territorial boundary.

d. Classified or National security information:

This type of data is considered sensitive to national security and thus requires additional safeguards. This type of Data must reside only on-premise of the public institutions or collocated or in a cloud within the Nigerian territorial boundary.

1.2.3. NITDA Guidelines for Nigerian Content Development in Information and Communication Technology (ICT) 2013

These guidelines cover subscriber and consumer Data hosted by telecommunications companies, network service companies, and ICT companies; and sovereign Data hosted by ministries, departments, and agencies of Nigeria's federal government and information management companies.[12] It requires data and information management companies to host all sovereign data[13] locally in Nigeria. The Guideline prohibits the transfer of Sovereign data outside the shores of Nigeria without NITDA's express approval making the cross-border transfers or hosting of sovereign data are permissible only with NITDA's express approval.[14]

The Guidelines have the following Data Localisation provisions:

Guideline 12.1(4) requires all ICT Companies to host all subscriber and consumer data in Nigeria.

[12] Guidelines 11.1(4), 12.1(4), 13.1(2), and 13.2(3), NITDA ICT Guidelines. https://nitda.gov.ng/wp-content/uploads/2019/08/NCCPolicy_New.pdf accessed on 20 June 2021

[13] Sovereign data in this sense means government data

[14] Lambo, Olayinka, Orabueze, And Eke-Opara, 'Data Localization Laws: Nigeria', Practical Law Data Privacy Advisor, https://www.uubo.org/media/1795/data-localization-laws-nigeria-w-022-1015.pdf accessed on 20 June 2021

Guideline 13.2(1) mandates all MDAs of Nigeria's Federal Government to host their websites locally and under a registered .gov.ng domain.[15]

Guideline 14.1(2) & (3) requires all Data and information management companies to host all sovereign Data in Nigeria and ensure compliance within 18 months from the publication of these guidelines.

1.2.4. CBN's mandatory 2011 Guidelines on Point of Sale (POS) Card Acceptance Services:

The Guidelines prohibits the routing of transactions outside Nigeria for switching between Nigerian issuers and acquirers. It also mandates entities engaging in point of sale (POS) card acceptance services in Nigeria to use a local network switch for all domestic POS and ATM transactions.[16]. The Guidelines cover all domestic transaction data of cardholders in Nigeria. A cardholder is any person issued a payment card whose account will be debited to settle transactions performed with the payment card.[17] The POS guideline is, however, silent on Cross-border transfer of data.

1.2.5. Absence of penalties for violation:

Although the Data Protection bill 2019 placed a very harsh penalty on violation of its data localisation provisions, the Guidelines on Point of Sale (POS) Card Acceptance Services, the NITDA ICT Guidelines and the National Cloud Computing Policy do not specify any penalties for violations. This makes enforcement of these laws very theoretical and challenging.

1.3. Reasons for Data Localization

a. Geopolitical Concerns

Governments view data localisation to ensure the safety and protection of data in the event of a global geopolitical crisis. For instance, a significant amount of cross-border data flow is managed through

[15] Lambo, Olayinka, Orabueze, And Eke-Opara, 'Data Localization Laws: Nigeria', Practical Law Data Privacy Advisor, https://www.uubo.org/media/1795/data-localization-laws-nigeria-w-022-1015.pdf accessed on 20 June 2021
[16] Guideline 4.4.8 POS Guidelines
[17] Guideline 4.4.8 and Appendix 1(b), POS Guidelines.

undersea cables. Data Localisation is viewed as a concern because the location of almost every undersea cable in the world is publicly available.

b. Foreign Surveillance

A significant reason for data localisation is to prevent foreign surveillance. There is a belief, albeit erroneous, that preventing personal information, emails and other forms of data from leaving the country would curb foreign surveillance and protect citizens' online privacy.

c. Data Localisation may help local law enforcement in tackling cybercrime.[18]

Cybercrime investigation is notoriously difficult since the Act involves multiple jurisdictions at once. It is presumed that storing data in a foreign jurisdiction, where domestic law enforcement does not have access or capacity, may impede the performance of duties of law enforcement agencies. These challenges could render cybercrime investigation ineffective.[19] Thus, making Data Localization an easier policy option for some states to protect law enforcement. However, this argument is flawed as Cybercrimes is transnational in nature and mandating the location of data centres within the country does very little in the war against cybercrimes.

d. Economic Development and Exploring Analytics:

There is a belief that localising Data within national borders will increase investment locally. The above is known as "Data mercantilism"[20], an open government policy to promote economic advantage by favouring local industries. Data Localisation measures are often motivated, whether explicitly or not, by promoting domestic economic development. Azmeh and Foster[21] highlight the benefits of a Data Localization policy for developing countries to include increased foreign direct investment in digital

[18] Neha Mishra, 'Data Localization laws in a digital world: Data protection or Data protectionism,' (2016) The Public Sphere 135, 150.
[19] John Selby, 'Data Localization laws: trade barriers or legitimate responses to cybersecurity risks or both?' (2017) 25 International Journal of Law and Information Technology 213, 214.
[20] Localization Barriers to Trade: Threat to the Global Innovation (2013), ITIF., http://www2.itif.org/2013-Localization-barriers-to-trade.pdf. accessed on 20 June 2021
[21] Shamel Azmeh,. and Christopher Foster, 'The TPP and the digital trade agenda: Digital industrial policy and Silicon Valley's influence on new trade agreements', (2016), Working Paper. International Development, Working Paper Series (16-175). Department of International Development http://eprints.whiterose.ac.uk/125522/ accessed on 20 June 2021

infrastructure and positive spill-over effects of an indigenous market for Data centres through enhanced connection, job creation and the presence of skilled professionals.[22]

e. National Security

National Security is perhaps the Government's most persuasive case for Data Localization. Data Localization is also considered a step towards national security because it can act as a barrier to preventing foreign surveillance and illegal data breaches. If data servers with critical personal servers were stored abroad, it is feared that it would allow foreign governments to infringe upon the privacy and security of such data. National Security appears to be a legitimate concern due to the rise of cyber terrorism and cyber espionage by state and non-state actors, heightened the concern for the security of data stored outside a country's borders.

f. Taxation

Another key argument for Data Localization is the taxation of foreign companies on the income generated through processing citizens data. This argument is supported by the view that hosting local servers within a country's borders gives foreign businesses a "fixed place of business", hence bringing such multinationals within the tax net. The Finance Act 2019 has rendered this unnecessary by introducing the concept of Significant Economic Presence (SEP) to expand the scope of taxing foreign companies deriving income from their activities in the country, which were hitherto not captured within the tax net. The CIT (Significant Economic Presence) Order provides clarification on the concept of SEP for multinationals carrying on business or providing services to customers in Nigeria, under Section 13(2)(c) and (e) of CITA.[23] The Order states that a foreign company shall have a Significant Economic presence in Nigeria in any accounting year, where it derives N25 million annual gross turnover or its equivalent in other currencies from any or combination of the digital activities listed in

[22] Data as a Tool for Diplomacy in India - JURIST .... https://www.jurist.org/commentary/2020/05/akshat-agarwal-data-localization-india/ accessed on 26 June 2021.

[23] FGN Issues CIT (Significant Economic Presence) Order, [20 June 2020]. https://home.kpmg/ng/en/home/insights/2020/06/minister-of-finance-issues-order-on-significant-economic-presence-by-non-nigerian-companies.html accessed on 20 June 2021

the Order."[24] From the above, it is apparent that mandating the localisation of data in Nigeria might widen the tax net to include multinationals who do not have physical offices in Nigeria but who process personal data generated in Nigeria as they will be forced to process data locally in physical offices.

1.4. Challenges of Data Localization

While there are various strong arguments in favour of Data Localization, these benefits come at a considerable cost. Data Localisation raises several concerns and challenges. They include

1.4.1. Economic Impact

The European Centre for International Political Economy has found that localisation measures will cost countries such as China, Indonesia, Brazil, India and Vietnam between 0.2% to 1.7% of GDP and 0.5% to 4.2% in domestic investment.[25] If businesses no longer consider the costs of storing data locally to be worth the benefits it gets in return, it may lead to their exit from the country. Even the European Union is not left out as the study also found that localisation regulations cost EU citizens an estimated $193 billion per year, due in part to higher domestic prices.[26]

According to another study, storing data locally in Nigeria will cost about 0.2% to 4.2% in domestic investment.[27] In the long run, data localisation policies may adversely affect the Nigerian economy and generally place the economy at a disadvantage.

1.4.2. Organisational Cost

Data localisation may also raise costs for Nigerian businesses and consumers.[28] Data localisation will require more significant investment in terms of time, cost and new infrastructure. This may lead to financial strain for businesses, especially start-ups who rely on leasing or renting server space from larger enterprises that are more often than not in foreign jurisdictions to develop new technologies and

[24] Ibid
[25] Ibid
[26] ECIPE, 'The costs of Data Localization: friendly fire on economic recovery', http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf. accessed on 20 June 2021
[27] Nwosu Data Localization: The Effects on Cloud-Adoption in Nigeria https://ssrn.com/abstract=3065432 accessed on 20 June 2021
[28] Ibid

sell services and products. Local data storage costs are higher than global systems, which operate at scale. It costs about $0.15 per GB for 0-5 TB of cloud space and even less as sizes get bigger on Go4hostina[29], an Indian web hosting service and about $0.10 per GigaByte (GB) standard Cloud service on Microsoft Azure[30].

To cushion the effect of the increased cost on the business, the additional cost will be passed on to customers, thus making services more expensive for customers.[31] With laws that allow organisations to move data in and out of a country freely, businesses can leverage affordable global cloud services, thus improving the ease of doing business in Nigeria.

1.4.3. Data Security:

Data localisation may also inadvertently raise the risk of security breaches as companies are forced to use local service providers that may not provide the best services available. Local data centres will also be a treasure trove for hackers and cybercriminals, leaving such centres vulnerable and susceptible to cyber attackers. The physical centralisation of data creates a "jackpot" problem for organisations because a hacker only needs to hack a few servers to access its user's data.[32] Security is not enhanced just because data resides within a particular jurisdiction. Security is a function of an entity's technical, organisational, and financial capacity to protect the data and provide physical protection for a data centre.[33]

1.4.4. The structure of the Internet:

In terms of internet technology, data localisation violates the original intention of internet design and undermines the open and interoperable internet architecture. One Internet, the final report published by the Global Commission on Internet Governance in June 2016, indicated that the data transmission on

[29] https://go4hosting.com/ng/cloud-storage.htm accessed on 20 June 2021

[30] https://azure.microsoft.com/en-us/pricing/ accessed on 20 June 2021

[31] 'Data Localization in A Globalised World: An Indian Perspective' - The Dialogue.

[32] Irfan, "Data Flows, Data Localization, Source Code: Issues, Regulations and Trade Agreements" . Geneva: CUTS International, Geneva. 2019

[33] Data Processing and Security Terms | Google Cloud Platform Terms ...." 7 February 2017, https://cloud.google.com/terms/Data-processing-terms-20170207. accessed on 20 June 2021

the Internet follows the principle of efficiency and does not consider border factors.[34] According to the report, regional restrictions imposed on data transfer will "shake the stability of the Internet infrastructure".[35] Some authors believe that the data localisation measures may conflict with developments in information technology development like big Data, and the Internet of Things (IoT) and cloud computing.[36]

1.4.5. Global Trade:

The free mobility of data is crucial for global trade. Under Article 15 (c) (ii) of Protocol on Trade in Services of the AcFTA, the protection of privacy of individuals concerning the processing, dissemination and protection of confidentiality of individual personal data is an exception to restraint on trade.[37] Article XIV (c) (ii) of the World Trade Organisations (WTO) General Agreement on Trade in Services (GATS) also permits trade restrictions when they are necessary for the protection of privacy of individuals concerning the processing, dissemination and protection of confidentiality of individual personal data and when such measures do not amount to "arbitrary or unjustifiable" discrimination between countries or a disguised restriction on trade and services".[38] Strict adoption of data localisation policies may appear "unjustifiably discriminatory" against other countries. While the potential need to control cross-border flows of data for privacy purposes is clear, applying such controls in an increasingly interconnected world is challenging.[39]

[34] Global Commission on Internet Governance: One Internet, 21 June 2016, P36, https://www.ourinternet.org/report accessed on 20 June 2021

[35] Ibid at Page 55.

[36] Anupam Chander and Uyen P. Le, 2014, Breaking the Web: Data Localization vs. the Global Internet, UC Davis Legal Studies Research Paper No. 378, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407858 accessed on 20 June 2021

[37] Oloyede Ridwan, "The Africa Continental Free Trade Agreement and Cross-Border Data Transfer: Maximising The Trade Deal in The Age of Digital Economy" 20 March 2019.

https://aanoip.org/the-africa-continental-free-trade-agreement-and-cross-border-data-transfer-maximising-the-trade-deal-in-the-age-of-digital-economy/ accessed on 20 June 2021

[38] UNCTAD, "Data protection regulations and international data flows: Implications for trade and development" https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf accessed on 20 June 2021

[39] UNCTAD, "Data protection regulations and international data flows: Implications for trade and development" https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf accessed on 20 June 2021

1.4.6. Financial Services:

The Financial Services industry is mainly dependent on data. Total investment activity globally in Financial technology reached a peak of US$120bn in 2018, up from US$51bn in 2017.[40] WeeTracker reports that Nigerian fintechs, including internationally headquartered companies that have invested in Nigeria, raised US$679m in 2019.[41] The Fintech sector is a growing sector reliant mainly on cross-border data, and data localisation policies may cripple this emerging sector.

1.5. Alternatives to Data Localisation

A.	**Policy Alternatives**	
	Mandatory Sectoral Localisation	**Conditional ('Soft') Localisation**
	In place of a generalised localisation requirement, it may be more utilitarian to identify sectors or categories of Data that may require local storage and restrict localisation within those sectors.	The Government should develop conditional precedents and standards for transferring all kinds of Data to any jurisdiction. These conditions can be: ● Equivalent privacy and security safeguards ● An agreement to share personal data with law enforcement officials when necessary: This appears to be the current position of the law in Nigeria. The NDPR and the NDPR implementation framework preclude any transfer of Data to any country that does not provide an adequate level of protection as determined by NITDA and the Attorney General of the Federation.[42] Where a transfer to a jurisdiction outside the whitelist is sought, the data controller is mandated to ensure there is verifiable documentation of consent to one or more of the exceptions stated in Article 2.12 of the NDPR.

[40] "The Pulse of Fintech H1'19: Biannual global analysis of investment in fintech", KPMG, July 31st 2019. https://home.kpmg/au/en/home/campaigns/2019/07/pulse-of-fintech-h1-19-global-trends.html accessed on 20 June 2021

[41] State of play: Fintech in Nigeria State of play: Fintech in Nigeria, The Economist Intelligence Unit Limited 2020

[42] Article 2.11 of the NDPR

B.	Incentivising Data Storage		
	Tax Incentives	**Robust Infrastructure**	**Legal Security of Data**
	Federal and State governments in Nigeria can give tax incentives to companies that operate data centres in Nigeria, thus making it lucrative and attractive to organisations to invest in Nigeria's Data centre industry.	More excellent internet and ICT availability, accessibility, and affordability should be given priority by the Government to encourage data storage in Nigeria. The World Bank, in a study using Data from 2001 to 2013 to measure the impact of internet penetration on bilateral trade, they concluded that with an insight that a 10% rise in internet penetration in the exporting country drives a 1.9% increase in the number of goods exported. Similarly, a 10% rise in internet penetration in the importer led to a 0.6% increase in the average value of goods[43]. This shows the vital role robust ICT infrastructure play in a nation's economy.	Unless the State can guarantee that data stored within its geographic territory is secure through a legal process, it will be difficult for multinationals to trust that data that is stored locally will be safe. The Government must enforce existing laws and enact laws that protect and secure the legal status of Data residing and stored within Nigeria. This is one of the reasons the NDPR was such a welcome development. The Passing of the Data Protection Bill 2020 will also be crucial to increasing the faith of organisations that set up Data centres in the safety of their Data within Nigeria.

[43] "World Bank Document - Open Knowledge Repository." https://openknowledge.worldbank.org/bitstream/handle/10986/24866/WPS7785.pdf. accessed on 20 June 2021

1.6. Data Localisation around the world

Rwanda

Rwanda has developed a Data Revolution Policy (DRP)[44] to be executed over five years from 2017 to 2022. The stated vision of the Rwandan Government is to build an innovation-Data-enabled industry to harness rapid social-economic development.[45] The policy contains a series of legal, policy and regulatory instruments addressing different aspects of digital trade. It provides that all critical information Data within the Government should be hosted in one central national data centre.[46] The policy, however, allows sovereign Data to be hosted in a cloud or a co-located environment in Data centres within or outside of Rwanda, only under agreed terms and governed by Rwandan laws.[47] In 2020, a Draft Data Protection law for Rwanda was unveiled, and it contained data localisation provisions.[48] Article 55 clearly states that "Any controller and/or processor shall host and/or store the data in Rwanda". Article 52 also prohibits the remote access of data by the data controller from another country without the authorisation of the Data Protection Authority. Article 46, however, prohibits the confinement of non-personal data unless such confinement is justified on the ground of National security and Article 54 permits cross-border flows of personal data on various bases listed in the Bill.

Kenya

When the 2018 draft of the Data Protection bill was released, it was met with protests by various stakeholders within the Kenyan data protection sector.[49] One of the reasons for the condemnation of the Bill was that it had a requirement for "the storage, on a server or data centre located in Kenya, of at

[44] National Institute of Statistics of Rwanda http://statistics.gov.rw/publication/rwanda-national-Datarevolution-and-big-Data accessed on 20 June 2021
[45] Ministerial Order No. 001/MINICT/2012 of 12 March 2012
[46] Irfan, "Data Flows, Data Localization, Source Code : Issues, Regulations and Trade Agreements" . Geneva: CUTS International, Geneva. 2019
[47] Ibid
[48] Rwanda Draft Data Protection Law 2020 available at https://www.dataguidance.com/sites/default/files/30802b_965abe73ea2e48899a28a4aefe2d3705.pdf accessed on 26 June 2021.
[49] In its comments on the Bill, the United states condemned these measures stating that it would "raise costs for firms, especially foreign firms, which are more likely to depend upon data centres located outside Kenya". Comments by the United States to Kenya's Ministry of Information, Communications and Technology on its Draft Data Protection Bill, 2018, https://ca.go.ke/wp-content/uploads/2019/01/U.S.-Government-Comments.pdf accessed on 20 June 2021

least one serving a copy of personal data to which this Act applies."[50] The Bill also prohibited the processing of sensitive personal data outside Kenya.[51] The Kenya Data Protection Act 2019 took a slightly different approach by providing that sensitive data can only be processed outside Kenya if the consent of the data subjects is obtained.[52] The Act empowers the Cabinet secretary to restrict the processing of data of a particular nature to servers or data centres located in Kenya on the grounds of strategic interests of the State or protection of revenue.[53]

South Africa

It appeared that South Africa operated a conditional cross border transfer regime by imposing some conditions for data flow. This was because the Protection of Personal Information Act did not impose any data localisation or residency requirements. However, on 1 April 2021, the Department of Communications and Digital Technologies published the Draft National Data and Cloud Policy (GG No. 44389).[54] The draft policy provides that:

- All data classified/identified as critical Information Infrastructure shall be processed and stored within the borders of South Africa;
- Cross-border transfer of citizen data shall only be carried out in adherence with South African privacy protection policies and legislation (POPIA), the provisions of the Constitution, and in compliance with international best practise;
- Notwithstanding the policy intervention above, a copy of such data must be stored in South Africa for law enforcement.[55]

Although this policy is still a draft that is yet to come into force, there has been much push back against the adoption and subsequent implementation of the data localisation provisions in the policy.

[50] Section 44 (1) of the Draft Data Protection Bill 2018.
[51] Section 44 (3) of the Draft Data Protection Bill 2018
[52] Section 49 of the Kenya Data Protection Act 2019 available at http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf accessed on 26 June 2021
[53] Section 50 of the Kenya Data Protection Act 2019
[54] https://www.gov.za/sites/default/files/gcis_document/202104/44389gon206.pdf accessed on 20 June 2021
[55] Paragraph 10.4 of the Draft National Data and Cloud Policy (GG No. 44389)

Russia

Russia's Federal Law No. 242-FZ came into effect in September 2015[56]. The legislation compels organisations to "gather, store, and process the Personal Data of its residents using the Data servers located in the country"[57]. The Regulation mandates personal data operators to process the personal data of Russian users in Databases within Russia and inform Russian authorities of the location of these data centres.[58] In addition, the law provides government institutions with more effortless access to information and imposes harsh penalties on non-compliant organisations.[59] The law also restricts Russian users from accessing any website that violates the nation's Data protection laws.[60]

China

China introduced a comprehensive Data Localization law in 2017.[61] The law forbids banks and other financial institutions from storing any personal financial data that they collect in China abroad. It also requires service providers to store any 'important Data' collected within China unless they pass a security assessment.[62]. Article 37 of China's Cybersecurity Law mandates "critical information infrastructure" operators to store all personal information produced within the mainland territory within mainland China.[63]

India

India has also enacted a range of laws and regulations requiring Data Localization. In 2012, India enacted a "National Data Sharing and Accessibility Policy," which provides that government data must

[56] Russia Data Localization Requirement at a Glance - Bryan Cave Data ...." http://bryancaveDatamatters.com/wp-content/uploads/2015/05/Russia-Data-Localization-Requirement-at-a-Glance.pdf. accessed on 20 June 2021
[57] Federal Law No. 242-FZ. | wilmap." 14 May. 2018, https://wilmap.law.stanford.edu/entries/federal-law-no-242-fz. accessed on 20 June 2021
[58] Bauer, Makiyama, Verschelde, "Data Localization in Russia: A Self-imposed Sanction" No. 6/2015
[59] Ibid
[60] Ibid
[61] Y. Wei, Chinese Data Localization Law: Comprehensive but Ambiguous, 7 February 2018, https://jsis.washington.edu/news/chinese-Data-Localization-law-comprehensive-ambiguous/ accessed on 20 June 2021
[62] Chinese Data Localization Law: Comprehensive but Ambiguous, February 7 2018, https://jsis.washington.edu/news/chinese-Data-Localization-law-comprehensive-ambiguous/. accessed on 20 June 2021
[63] Ibid

be stored in local Data centres. In 2019, The Indian Data Protection Bill was introduced in parliament, and it is still being debated. The Bill introduces the first economywide data localisation requirement for specific categories of data (sensitive personal data).[64] This is in addition to various sector-specific localisation requirements that already exist. For example, the telecoms regulators local storage of subscriber information and prohibits the cross-border transfer of same, the Companies (Accounts) Rules law 2014 provision that requires financial information if primarily stored overseas, to be backed up with storage in India. The Reserve Bank of India (India's Central bank) recently mandated the storage of payments data in India even if the processing is carried out outside India.[65]

European Union (EU)

The General Data Protection Regulation (GDPR) (REGULATION (EU) 2016/679 came into force in 2018. The GDPR operates a conditional transfer approach based on a determination of adequacy. According to Article 45 of the GDPR, Personal Data may only be transferred to a country, organisation or territory that provides an 'adequate level of protection. The European Commission makes such assessments of adequacy, considering factors such as the respect for human rights, the rule of law, and the presence of an independent supervisory authority. On 23 January 2019, the European Commission announced its adequacy decision regarding Japan,[66] the first adequacy decision since the Regulation's entry into force.[67] The European Commission has granted Adequacy decisions to Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New

[64] Burman and Sharma, "How Would Data Localization Benefit India?" Carnegie India, 14 April 2021. https://carnegieindia.org/2021/04/14/how-would-data-localization-benefit-india-pub-84291 accessed on 23 June 2021.

[65] FE Online, "RBI reiterates its stand on data localisation; says, payment data of Indian customers to remain in India", 26 June 2019, https://www.financialexpress.com/economy/rbi-reiterates-its-stand-on-data-localisation-says-payment-data-of-indian-customers-to-remain-in-india/1619933/ accessed on 23 June 2021.

[66] Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal Data by Japan under the Act on the Protection of Personal Information (hereinafter, the "EU-Japan Adequacy Decision"), available online at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.076.01.0001.01.ENG&toc=OJ:L:2019:076:TOC. 20 June 2021

[67] Gerlach and Keustermans, "Europe and Japan towards the Future – the first post GDPR adequacy decision of the European Commission"

Zealand, Switzerland, and Uruguay (not in this Order).[68] On 16 June 2021, the Commission also announced the procedure for adopting an adequacy decision for South Korea under the Regulation.

While the European Union does not mandate data retention within its territory, it has been argued that imposing a complex set of conditions that must be complied with for cross border transfers of Data acts, in effect, as a mandate for localisation.[69] Controllers may find it easier and cheaper to store data within the European Union rather than navigate the complex requirements imposed by the EU or risk falling short of compliance.[70]

In November 2018, the European Parliament and Council passed the Regulation (EU) 2018/1807.[71] The Regulation prohibits Data Localization and establishes the free flow of non-personal data from the Member States. Local storage may be mandated only on the grounds of public security, and any Data Localisation mandates must be communicated to the European Commission to ensure compliance. [72]

African Regional and Subregional instruments

It is worth noting that the African Convention on Cybersecurity and Personal Data Production (Malabo Convention)[73] does not contain any provisions on cross-border transfer of data. On the plus side, the Malabo convention doesn't contain Data localisation requirements either. On the other hand, the Economic Community of West African States (ECOWAS) has adopted the adequacy approach to data movement across borders. The ECOWAS Supplementary Treaty on Personal Data Protection provides that "The data controller shall transfer personal data to a non-member ECOWAS country only where

[68] "Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection", https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en accessed on 26 June, 2021.
[69] Chander and Le Anupam Chander, Uyên P. Lê, Data Nationalism, 64 Emory L.J. 677 (2015), http://law.emory.edu/elj/content/volume-64/issue-3/articles/Data-nationalism.html accessed on 20 June 2021
[70] Ibid
[71] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal Data in the European Union https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1546942605408&uri=CELEX:32018R1807 accessed on 20 June 2021
[72] Ibid
[73] https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf accessed on 26 June 2021

such a country provides an adequate level of protection for the personal data of individuals".[74] The Southern African Development Community (SADC) Model Law on Data Protection adopts a similar approach as the ECOWAS Supplementary Act but breaks the requirements down into movement within the SADC and outside the SADC.[75] The subregional instruments appear not to discourage data movement across jurisdictions if adequate security measures exist in the recipient nation. However, while the ECOWAS act is binding on member states, the SADC model law is not in force at the moment.

Conclusion

The ability to share data is as crucial as data itself. It is apparent that when it comes to mandatory localisation of data, the challenges outweigh the benefits. This article has outlined the arguments for and against Data Localization and alternatives policy measures that the Government can explore to encourage local data storage rather than mandate it. In a digital economy, so much is dependent on the unencumbered movement of data around the globe. Data stands at the core of the 4th industrial revolution acting as the driving force of the revolution. To fully benefit from the 4th Industrial Revolution, it is time for nations to move away from the Localisation of Data towards Globalisation of Data.

ABOUT THE AUTHOR

Victoria Oloni is a Trainee Solicitor with Detail Commercial Solicitors, a Corporate Commercial law firm in Lagos, Nigeria. She works within the Digital Economy, Privacy, Data Protection and Cybersecurity sector. She has published several articles on various platforms, and her latest project is the Data Protection 101 podcast which she hosts on the DigiLaw Platform.

[74] Article 36 of the Supplementary Act A/SA.1/01/10 On Personal Data Protection Within Ecowas available online at https://www.statewatch.org/media/documents/news/2013/mar/ecowas-dp-act.pdf accessed on 26 June, 2021.

[75] Article 43 and 44 of the Southern African Development Community (SADC) Model Law on Data Protection, https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf accessed on 26 June 2021.

AFRICAN
ACADEMIC NETWORK
ON INTERNET POLICY