POLICY BRIEF 08

MANDELA INSTITUTE

THE IMPACT OF DATA LOCALISATION LAWS ON TRADE IN AFRICA

Kholofelo Kugler

MANDELA INSTITUTE, SCHOOL OF LAW,
UNIVERSITY OF THE WITWATERSRAND

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG

CONTENTS

1. INTRODUCTION

Cross-border data flows have become an integral aspect of globalisation in the 21st century. In fact, almost every type of cross-border transaction has a digital component — the global economy has become increasingly data dependent. The free flow of data has unlocked innovation in all economic sectors: from boosting healthcare advances to facilitating greater automation in manufacturing. As a result, global consumers have come to expect instant and on-demand services that are enabled by access to datasets of great size and at great speed.[1]

While transnational data flows transmit valuable streams of information and ideas in their own right, they are also key enablers of flows of goods, services, capital, and people. A 2016 McKinsey study noted that cross-border data flows have raised global Gross Domestic Product (GDP) by approximately USD 2.8 trillion in 2014 (i.e., by 3%). This exceeds the USD 2.7 trillion generated by the global trade in goods in the same year. In just a decade, global data flows have generated as much economic value as trade networks that have been developed over centuries.[2]

> The free flow of data has unlocked innovation in all economic sectors

The COVID-19 pandemic has further highlighted the value of digital trade, which has grown since the beginning of 2020, even when global GDP growth rates were plunging.[3] Free data flows are critical to the management of the pandemic and concomitant public health measures. Timely and unhindered access to data have ensured adequate economic and health responses, as well as social connections between people via social networks and video calling applications.[4]

However, paradoxically, the global adoption of cross-border data restrictions, particularly data localisation requirements, is increasing. The number of countries that have adopted these requirements has grown from 35 in 2017 to 62 in 2021. The total number of data localisation restrictions has more than doubled from 67 in 2017 to 144 in 2021. Another 38 policies have been considered or proposed globally. China (29), India (12), Russia (9), and Turkey (7) are the leaders in requiring forced data localisation.[5]

This trend has not missed Africa as some African countries have already adopted or are considering adopting data localisation requirements. This paper assesses the impact of data localisation requirement on trade in Africa and is organised into six sections. After the introduction, the second section explains the general modalities and reasons for adopting these measures. The third section highlights the types of cross-border data flow restrictions and prohibitions that African countries have adopted. The fourth section discusses the economic and trade impacts of data localisation requirements in Africa. The fifth section explores the ways in which the effects of data localisation restrictions could be cushioned by the various international and regional trade obligations that African countries have undertaken. Finally, a brief conclusion is provided in the sixth section.

2. DATA LOCALISATION REQUIREMENTS: MODALITIES AND REASONS

There are generally three main types of data localisation requirements. First, governments restrict the transfer of data outside their borders (strict data localisation requirements). Second, governments restrict data considered sensitive or related to national security. Third, governments permit cross-border data flows based on the fulfilment of certain conditions (conditional flow regimes). An example of a conditional flow regime is the General Data Protection Regulation (GDPR) of the European Union (EU).[6] However, at times, conditional flow regimes can be de facto data localisation requirements because the cost of compliance is so high and difficult that firms have no other option but to store data locally, especially when faced with large financial penalties.[7]

Countries generally adopt or plan to adopt data localisation requirements for the following reasons:

- To ensure data privacy, protection, and cybersecurity;
- To support local law enforcement by ensuring that local authorities have access to the data needed to investigate crimes;
- For government censorship and surveillance;
- To mitigate geopolitical risk and financial sanctions; and
- For economic development purposes.[8]

As discussed in further detail in section 3, African countries have mainly adopted data localisation

requirements for data protection purposes. However, some have cited economic development desires, including job creation through growing the domestic local data processing industry for adopting or wishing to adopt these measures.

Before delving into the economic and trade impacts of data localisation requirements, an overview of African countries cross-border data restrictions, including data localisation requirements, is provided below. This is not an exhaustive account of every African country's cross-border data restriction regime but is rather illustrative, providing examples of how African countries generally regulate cross-border data flows. The data regimes of Kenya, Nigeria, and South Africa have already been discussed in detail in other papers in this series.

3. A BIRD'S EYE VIEW OF CROSS-BORDER RESTRICTION AND LOCALISATION REGIMES IN AFRICA

In light of the divergent international views on data localisation, African countries have adopted differing approaches to cross-border data restrictions. According to GSMA, there is about a 50-50 split between African countries that have adopted some sort of data flow restrictions and those that have not. Concretely, 26 African countries have no cross-border data flow restrictions; 26 have adopted conditional flow regimes (in other words, they permit cross-border data flows subject to contractual safeguards, prior authorisation, or adequacy decisions by authorities); and two African countries have no prior restrictions for data transfers but ex-post accountability for data exporters.[9]

Thus far, Nigeria is the only African country to explicitly adopt strict data localisation requirements for economic reasons. According to the Guidelines for Nigerian Content Development in ICTs established by Nigeria's National Information Technology Development Agency (NITDA), all government data and all subscriber and consumer data held by telecommunications companies may not be transferred outside of the country.[10] These measures were adopted to address Nigeria's negative trade balance in the information technology sector.[11] This would be achieved by requiring the use of local Nigerian content to incrementally add domestic value to information and communications technology (ICT) products and services. The actual measures include developing local skills/skills transfer; technology transfer; using domestic labour and developing local manufacturing.[12]

In April 2021, South Africa published its draft National Policy on Data and Cloud of 2021[13] for comment. In this policy, the South African government seeks to adopt strict data localisation requirements for economic development objectives. This policy has not yet been adopted but, if adopted without substantial changes to the text, it will likely have a profound impact on the South African economy, including cross-border trade.

Other African countries have adopted strict data localisation requirements for data protection purposes. For example, section 70(1) of Zambia's Data Protection Act of 2021 prohibits the cross-border transfer of personal data. In Kenya, the Data Protection Act of 2019 restricts the cross-border transfer of 'public data' without prior authorisation. Other countries like Chad,[14] Senegal,[15] South Africa,[16] Tunisia,[17] Uganda[18], and Zimbabwe[19] have adopted conditional flow regimes for data protection purposes.

African countries have also adopted sector-specific restrictions. For instance, Nigeria,[20] Uganda,[21] and Rwanda[22] have adopted restrictions in financial services. Rwanda,[23] Zambia,[24] and Zimbabwe have adopted restrictions to prevent cybersecurity and cybercrimes. Moreover, Rwanda[25] and Nigeria[26] (as reflected above) have adopted restrictions in telecommunications.

> African countries have adopted differing approaches to cross-border data restrictions

However, information on enforcement mechanisms (i.e., whether the respective countries have issued the relevant authorisation or enforced regulatory sanctions) and the capacity of local data processors to protect citizen's privacy rights is scant. There are also increased concerns that data localisation requirements could facilitate state surveillance activities as African states would not need to go through foreign countries or intermediaries to access their residents' data.[27]

A rather exceptional case of African countries' enforcement of data localisation requirements is Rwanda's enforcement of its telecommunications licence conditions in 2017. Rwanda's telecommunications regulator, Rwanda Utilities Regulatory Authority, fined MTN Rwanda (a subsidiary of South Africa's MTN Group) USD 8.5 million (10% of its annual turnover) for failing to comply with a licence condition to process Rwandan customer data in the country, by transferring it to Uganda and for running its information technology services outside the country.[28] This is a clear example that data localisation requirements do not only exist in legal

instruments but can be contractual or part of licensing requirements. It also underscores the great financial burden that multinational (and local) companies might face if they do not (or cannot) comply with data localisation requirements, even in markets as small as Rwanda's. Rwanda has since adopted a general data protection law in 2021, which seems to be more flexible than the requirement imposed on MTN. Pursuant to Article 48, cross-border data transfers are conditional upon authorisation of the relevant authority, consent of the data subject, necessity, and for compliance with Rwanda's international obligations.[29]

The United States Trade Representative (USTR) has noted the data restrictions or localisation requirements that Nigeria and Kenya have adopted. The measures adopted by these two African countries are the only ones that have been raised by the United States (US) government thus far. According to the USTR, these measures, respectively, 'discriminate against foreign businesses that distribute their data storage and processing globally'[30] and, in the case of Kenya, 'will hamper the development of Kenya's digital economy, and may undermine data security without providing any meaningful benefit to data privacy'.[31]

4. THE ECONOMIC AND TRADE IMPACT OF DATA LOCALISATION REQUIREMENTS IN AFRICA

4.1. Debunking the myth of economic gains from data localisation requirements

For many years, data has been referred to as 'the new oil'. This analogy sought to communicate the value of this resource and its centrality in innovation and the global economy. However, this catch phrase has also contributed to a flawed understanding that the best way to reap the economic benefits of data is to hoard it behind a country's borders. Data's value is maximised when it can flow with trust and permission across economic sectors and national borders. Therefore, optimal data policies are those that allow the flow of data in a way that ensures safety, security, and equal access. [32]

This understanding of data as a commodity that must be controlled in-country to maximise economic benefits has contributed to the proliferation of data localisation requirements. It has also informed South Africa's framing of data 'ownership' as a pathway to economic development in its proposed National Policy on Data and Cloud of 2021. While it is laudable that African governments are seeking greater privacy, security, and economic opportunities for their citizens, data localisation requirements could result in unintended consequences and great costs across the entire economy.

Data localisation, like most protectionist measures, results in marginal gains for a few local enterprises and workers, while causing significant economy-wide harm. Currently, the majority of Africa's data centres are privately owned. The main companies providing data processing/management services are MainOne (MDXi) (Ghana and Nigeria); Teraco Data Environments (South Africa); Liquid Intelligent Technologies Group (Africa Data Centres) (Kenya, Nigeria, and South Africa); and Orange (Cameroon, Côte d'Ivoire, Egypt, and Senegal).[33] The domestic benefits of data localisation would accrue to the few owners and employees of data centres and the few companies that service these centres locally. On the other hand, small, medium, and large businesses will suffer the negative consequences of limited or lack of access to data.[34]

> Imposing data localisation requirements to address public policy and economic development objectives is not necessarily the best way to achieve these goals

In any event, data that is stored locally as a result of data localisation requirements would not result in economic growth without the necessary open data and data access policies. In addition, local data processors would also be similarly constrained by the domestic data transfer requirements in order to comply with, for example, data protection requirements.

Governments implementing or contemplating data localisation requirements to boost local economies imagine that these measures will amount in enormous domestic economic benefits. Policy makers consider that the various global service providers operating in their country would build infrastructure locally. However, this is rarely the case. In fact, many service providers would find it uneconomical and even too risky to establish local servers in certain countries. The fact is: building, operating, and maintaining data centres is expensive.[35]

Even if multi-national companies established in-country data centres, these centres are not significant generators of employment because processes are generally automated, requiring limited human involvement to ensure that everything is operating

optimally. Furthermore, large data farms consume a large amount of energy and often further burden overtaxed energy grids.[36] Given the energy insecurity in even the most advanced African economies, creating a data processing economy is a massive undertaking. Under these conditions, the well-intentioned data localisation restrictions could force more innovative and price competitive firms to exit the market, allowing more expensive or inferior goods and services to capture more market share.[37]

> Data that is stored locally as a result of data localisation requirements would not result in economic growth without the necessary open data and data access policies

The Data Risk Index 'identifies the top risks likely to affect the successful operation of a data centre, and applies an individual weighting to those risks to create a balanced view and ranking of selected countries'.[38] The indicators assessed in this index are:

- Energy (cost per kWh);
- International internet bandwidth (Mbit/s);
- Ease of doing business (World Bank ranking)
- Corporation tax;
- Political stability (EIU's Instability Index);
- Sustainability (% energy from alternatives);
- Natural disasters;
- Energy security;
- GDP per capita; and
- Water (availability per capita).

Out of a sample size of 37 countries ranked in 2016, South Africa and Nigeria were the only African countries included in the survey. Based on an assessment of the above indicators, South Africa was ranked 30th and Nigeria last (37th).[39] This indicates that notwithstanding the desires of African policy makers, it is unlikely that global service providers would rush to establish data centres in even the most advanced African countries because the conditions in those countries are simply not conducive to this type of economic activity. Nevertheless, Amazon Web Services, Microsoft Corp's Azure and Huawei have recently established data centres in South Africa.[40] Huawei also plans to expand its data centre operations to other African countries.[41]

4.2. Findings on the economic and trade impacts of data localisation requirements

The trade and economic growth consequences of data localisation requirements and related data privacy and security laws were highlighted in 2014 by the European Centre for International Political Economy (ECIPE). ECIPE undertook to quantify these economic losses by using a computable general equilibrium model (CGE) called GTAP. While no African country was included in the study (which assessed the effects of recently proposed or enacted data localisation legislation in Brazil, China, the EU, India, Indonesia, South Korea, and Vietnam), the results were quite telling and can be expanded to the African context. ECIPE estimated that data localisation requirements could reduce GDP growth by up to 1.7% in the countries that they studied. The losses in total exports were felt most acutely in China and Indonesia, which suffered GDP losses of 1.7% resulting from data localisation requirements.[42]

In 2019, Badran and Tufail published an economic impact assessment of data localisation in Egypt, Kenya, Mauritius, Morocco, and South Africa. They evaluated macro-economic indicators based on sectoral production, imports and exports, based on ECIPE's methodology, to estimate the costs of data regulations.[43] The following is a summary of their findings on some of the broader economic impacts of restrictions to cross-border data flows in the five African countries:

- Overall estimates indicate that cross-border data transfer restrictions would result in a real GDP decline for all the countries studied, especially South Africa (owing to the country's dependence on service sectors that use data intensively), followed by Egypt. These results would be driven by a decline in private consumption (Egypt, Kenya, and South Africa) or a decline in investment (Mauritius and Morocco).
- All the countries would experience increases in production costs and a decline in income due to increases in prices of goods.
- The countries that were most impacted by changes in sectoral production include Egypt,

Morocco, and Kenya where 10 out of 15 sectors experienced declines. The least impact was found in South Africa.

- The sector most gravely impacted was construction, which is the fastest growing sector in Africa.[44]

Specifically related to international trade, the authors found an overall decline in imports in almost all the studied sectors and countries. The impact on imports, as opposed to exports, is more acute in Africa due to the import-dependency of African economies. The country most negatively affected by the trade impacts of data localisation requirements in this regard, was Morocco. Its manufacturing sector was particularly adversely affected.[45]

Restricting data flows would also undermine Africa's efforts to exploit the opportunities presented by e-commerce, which also relies on maintaining real-time data connectivity across the economy. Indeed, COVID-19 has accelerated the growth of e-commerce globally and preliminary research suggests that post-pandemic, the pace of e-commerce expansion will not contract.[46] With improved logistical infrastructure, and an enabling environment fostered by better trading conditions under the Agreement Establishing the African Continental Free Trade Area (AfCFTA), African countries could experience a boom in cross-border trade enabled by the internet. However, restriction on data flows could pose a threat to those aspirations.

4.3. Other impacts of data localisation requirements

Other costs of data localisation requirements include slowing down the digital infrastructure because of data segmentation and internet fragmentation thereby undermining fraud prevention and cybersecurity best practices because of weak domestic cybersecurity infrastructure in Africa. The best cybersecurity interventions are developed by experts in a few technology centres around the world. Unfortunately, enforcing data localisation would mean that African data processors may not have access to these tools. Other impacts of data localisation requirements include increased surveillance of private citizens by governments because of ease of access to data, which undermines their regulations on data privacy and significantly curbs democracy and human rights. In addition, insisting on data localisation might result in less privacy protection (more specifically, less protection of personal information) because of the above-mentioned weak domestic cybersecurity infrastructure.[47]

5. MITIGATING THE NEGATIVE TRADE IMPACTS OF DATA LOCALISATION REQUIREMENTS IN AFRICA

There is a general recognition that unfettered cross-border flows are not desirable or even warranted. Indeed, there are legitimate public policy reasons for governments to control the flow of data, including to protect privacy rights. However, in developing data transfer rules, African policy makers must adopt a risk-based approach. Some extremely sensitive data like that which is related to state security or some types of personal information including gender (which would be relevant for trans people) and sexual orientation (e.g., South Africa legally recognises and protects all types of gender and sexual identities) and health records that can be used to identify individuals may need to be controlled strictly. For state security-related data especially, the risks of cross-border sharing could exceed any likely economic or trade benefit. However, including additional controls, like requiring consent and anonymising personal information, could mitigate any potential negative consequences of transferring this type of data and result in economic or trade benefits. Hence, public and anonymised private data that would not harm states, individuals, or organisations can and should be transferred freely as the benefits of cross-border sharing would exceed any possible risks.[48]

> It is unlikely that global service providers would rush to establish data centres in even the most advanced African countries because the conditions in those countries are simply not conducive to this type of economic activity

These risk-based solutions could best serve those African countries that have not adopted any cross-border data restrictions or any data regulations at all. This approach might be ineffective for African countries that have already enacted data localisation requirements (although it might be possible for Data Protection Agencies to adopt a risk-based approach at the implementation stage or for governments to refine policies through subsequent regulations and policy instruments). Governments are unlikely to backtrack on these requirements as entire ecosystems of domestic beneficiaries with deeply entrenched interests have

already been established and it might be politically difficult to amend these laws. There are, however, possible solutions that can be explored outside individual countries that might mitigate the negative trade effects of data localisation requirements. These are discussed in turn below.

5.1. Multilateral commitments and possible commitments on cross-border data flows

Most African countries adopted their cross-border data restrictions in the past decade.[49] However, many of these countries have undertaken obligations under the General Agreement on Trade in Services (GATS), which pre-date their data transfer restrictions. In other words, to the extent that any African country's data localisation requirement is inconsistent with its obligations under the GATS, any World Trade Organisation (WTO) member can challenge the measure at the WTO's dispute settlement mechanism.

> In developing data transfer rules, African policy makers must adopt a risk-based approach

Article I:2 of the GATS defines cross-border trade in services as the supply of a service from one territory of a WTO member to the territory of another WTO member (Mode 1). Moreover, Article XXVII(b) of the GATS, includes in the definition of 'supply of a service' the 'production, distribution, marketing, sale and delivery of a service'. Therefore, the GATS contemplates the cross-border transfer of data as it relates to the production, distribution, marketing, sale, and distribution of a service. Moreover, the panel[50] in the WTO dispute *Mexico – Telecoms* confirmed that the supply of a service through Mode 1 occurs without the presence of the service supplier of a WTO member in the WTO member receiving the service.[51] In other words, the GATS contemplates the supply of services that does not involve the physical presence of a business entity in the country of service consumption. This underscores the fact that to the extent that data is involved in the cross-border supply of a service, the entity processing or otherwise utilising that data does not have to be present in the country of consumption.[52]

In addition, in the WTO dispute *US – Gambling*, the WTO Appellate Body confirmed that to the extent that a WTO member has undertaken to provide full market access under Mode 1 (in other words, has inscribed 'none' in the market access column corresponding to Mode 1), that WTO member may not prohibit the remote provision of a service, even if it permits the non-remote provision of the same service.[53] This essentially means that a WTO member that has undertaken full market access commitments under Mode 1 cannot restrict the cross-border supply of the service in any way. This is true even if a foreign company has a local presence that can provide a certain service, including the relevant data management to provide that service. This company may not be prevented from providing the related data from its parent or sibling entity that is outside of the country where the service is supplied.

Moreover, the panel in the WTO dispute *US – Gambling* confirmed that Mode 1 commitments cover the supply of services through electronic means like the internet.[54] Additionally, in the WTO dispute *China – Publications and Audiovisual Products*, the Appellate Body confirmed that GATS commitments – which largely pre-date the digital era – cover technological developments that were not contemplated at the time the commitments were undertaken.[55] Thus, even if at the time that members undertook their GATS commitments there was no internet banking, to the extent that a member had undertaken full financial services commitments under Mode 1, they would not be able to restrict internet banking, including the cross-border transfer of data necessary to supply the relevant banking services.

Nevertheless, Article XIV of the GATS contains general exceptions that WTO members can invoke for legitimate public policy purposes. Article XIV(c)(iii) expressly provides an exception for measures necessary to secure compliance with laws or regulations, including those relating to: 'the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts'. However, the use of, for example, data flow restrictions on privacy grounds should not amount to 'a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services'.

On the negotiations front, some WTO members are currently negotiating the Joint Statement Initiative on e-Commerce (e-Commerce JSI) that was launched on the side lines of the WTO Ministerial Conference in Argentina in 2017. Although the vast majority of African WTO members have chosen not to participate in these negotiations, Benin, Burkina Faso, Cameroon, Côte d'Ivoire, Kenya, and Nigeria are involved.

The latest publicly available draft consolidated text of this agreement was finalised in September 2021. The proposed Article 5 of section B.2. Flow of information: (1) [Cross-

border transfer of information by electronic means/Cross-border data flows] contains proposed provisions on the prohibition of data localisation.[56] This means that if this agreement is finalised, the data localisation requirements that are maintained by, for example, Nigeria, could be found inconsistent with this provision.

Henry Gao argues that WTO members could conclude a cross-border data flow agreement in the light of the ongoing e-Commerce JSI negotiations. These provisions could be included in the data flows section of the agreement. Gao postulates that the substantive elements of this agreement should include freedom of data flows; the prohibition of data localisation requirements, with narrowly defined exceptions to protect data security of personal information; and a commitment for each party to introduce or maintain its own domestic privacy laws that meet certain minimum standards.[57] This text will be binding on the African countries that ratify it and could mitigate some effects of the data localisation requirements adopted by those countries.

One of the 'certain minimum standards' that could be used is the Cross-Border Privacy Rules (CBPR) System of Asia-Pacific Economic Partnership (APEC) (APEC CBPR). The APEC CBPR is an accountability-based mechanism that facilitates privacy-respecting data flows. Private companies are required to implement compliant data privacy policies, including those on accountability, notice, choice, collection limitation, integrity of personal information, uses of personal information, and preventing harm. These companies are audited and certified by APEC-approved accountability agents. However, each APEC CBPR member country's data agency is responsible for enforcement. There are currently nine participating APEC CBPR system economies: the US, Mexico, Japan, Canada, Singapore, the Republic of Korea, Australia, Taiwan, and the Philippines.[58] Existing APEC CBPR could open the system to non-APEC members so that it can become a global model for data governance.[59] Alternatively, WTO members could adopt the system and create a centralised approval system at the WTO Secretariat.

5.2. Liberalising data flows regionally in Africa

The increase of data localisation requirements in Africa might have an unintended consequence on the trade liberalisation that is envisaged under the AfCFTA Agreement. While the AfCFTA e-commerce Protocol remains to be negotiated, the Protocol on Trade in Services (Services Protocol) came into effect in May 2019. Under Article 1(p) of this protocol, as long as it is technically feasible, services can be provided on a cross-border basis. These services would, of course, include data-enabled/supported services.

Therefore, any data localisation requirement could result in a violation of a number of provisions under the Services Protocol. For example, the most-favoured nation principle under Article 4 of the AfCFTA might be violated if a state party permits the transfer of data to another state party that it considers has adequate data protection laws, while it refuses the transfer to a country with similar data protections. In addition, there might be a violation of the national treatment obligation under Article 20 if the state party's data localisation requirement results in less favourable treatment for service providers of other state parties located in the state party imposing the measure because it is too costly for them to use local data centres or to establish their own. Like the GATS, Articles 15(c)(ii) and 15(c)(iii) of the Services Protocol, respectively, contain explicit data protection and safety exceptions that could provide a defence for a state party that implements measures taken for these purposes. However, data localisation measures taken for other purpose, for example, developing the domestic data processing sector, might be more difficult to justify.

> One way to facilitate regional data flows is for African countries to ratify the African Union Convention on Cyber Security and Personal Data Protection, 2014 (Malabo Convention)

One way to facilitate regional data flows is for African countries to ratify the *African Union Convention on Cyber Security and Personal Data Protection, 2014 (Malabo Convention)*.[60] Thus far, this convention has been signed by 14[61] African countries and ratified by eight.[62] The *Malabo Convention* could, inter alia, mitigate the effects of individual domestic data localisation requirements in Africa and provide a standard level of data protection that will prevent exclusion from accessing data from certain markets (in African and abroad) because of low levels of data protection and cybersecurity.

However, the *Malabo Convention* establishes a conditional flow regime under Article 14(6), which permits the transfer of data to non-African states if they have 'an adequate level of protection of the privacy, freedoms and fundamental rights of persons', unless the data controller obtains authorisation from the national data protection authority. This requirement would not apply to intra-Africa trade and it would probably not affect trade between trading partners like the US and the EU. However, it could create trade

barriers with trading partners that have, arguably, lower levels of freedoms and human rights, unless authorisation is obtained.

At the sub-regional level, ECOWAS member states have adopted the ECOWAS Supplementary Act on Personal Data Protection (2010) (ECOWAS Supplementary Act). It applies to, inter alia, data processing that is carried out in an ECOWAS and WAEMU member states. The ECOWAS Supplementary Act subjects data processors in the region to formalities that include declarations and authorisations to process certain types of data, including state data and personal data like biometric data, health information, and criminal records.[63] Further, Article 23 subjects the processing of personal information to the consent of the data subject. However, this consent may be waived for limited reasons, including to fulfil contractual obligations.

Furthermore, Article 36 of the ECOWAS Supplementary Act permits the transfer of personal data to non-ECOWAS countries where 'such a country provides an adequate level of protection for privacy, freedoms and the fundamental rights of individuals in relation to the processing or possible processing of such data'. The data controller must *inform* the data protection agency of this transfer. This provision could ostensibly imply that data controllers within, for example, Nigeria could transfer subscriber and consumer data that is covered by the localisation requirement outside of Nigeria. However, this can only occur if the third country has adequate rights protection in the area of data processing and the Attorney General of Nigeria is *informed* of this cross-border data transfer.

Finally, the Southern African Development Community (SADC) has issued a Model Law on Data Protection, which was adopted by the ministers responsible for Telecommunications, Postal and ICT services in 2012. Regarding data flows to non-SADC members, Article 44 also provides a mechanism for the flow of personal data upon, inter alia, the consent of the data subject or to fulfil contractual obligations between the data controller and a third party. However, this instrument is not binding on the parties and would not be useful in mitigating the effects of data localisation requirements in the SADC region.

5.3. Trade agreements with trade partners outside Africa

Thus far, no African country is party to the international agreements that have permissive data localisation regimes. These include the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), the United States–Mexico–Canada Free Trade Agreement (USMCA), and the Digital Economy Partnership Agreement (DEPA) between Chile, New Zealand, and Singapore. While no accession is possible to USMCA, African countries could request accession to the DEPA and the CPTPP but have not done so yet.

Nevertheless, most African countries are either negotiating or have concluded negotiations with the EU under the auspices of the Economic Partnership Agreements (EPAs). Currently, the following EPAs have entered into force: the EU–SADC EPA (implemented by Botswana, Eswatini, Lesotho, Mozambique, Namibia, and South Africa); the EU–Eastern and Southern Africa (ESA) EPA (implemented by Comoros, Madagascar, Mauritius, Seychelles, and Zimbabwe); the EU–Cameroon Interim EPA; and the EU–Côte d'Ivoire and EU–Ghana Stepping Stone EPAs.[64]

There are varying levels of data protection commitments in these EPAs. The EU–Cameroon Interim EPA, which entered into force in 2014, is the only one with a stand-alone data protection chapter. Under this agreement, the parties have agreed to process personal data in line with international standards.[65] They have also agreed to establish and maintain regulatory regimes and administrative capacity based on various principles, including purpose limitation, transparency, security, rights of access of the data subject, and restrictions of onward transfers. The parties have also agreed to keep each other informed of any international agreements that they conclude, particularly those that affect the collection, storage, and processing of personal data, as well as access by or transfer to third parties. This means that Cameroon must inform the EU of any data protection obligations it undertakes in the context of the AfCFTA or any other future trade agreements. Although the chapter generally sets out principles and is cooperative in nature, either party could initiate a dispute against the other party in the event of a breach. In the EU–Côte d'Ivoire Stepping Stone EPA, the parties have undertaken to negotiate provisions on the protection of personal data in the future.[66]

Moreover, in the EU–ESA EPA, the EU–Cameroon Interim EPA, and the Stepping Stone EPAs with Côte d'Ivoire and Ghana, data protection for the protection of privacy rights is listed as an exception justifying the violation of treaty obligations.[67] Other data protection obligations in all the EPAs include limited commitments in the area of customs cooperation where the parties agree to transfer data between each other based on the EU's equivalence approach.[68]

It is unclear why the EU has taken such an inconsistent approach to data protection in the various EPAs. However, as these agreements are subject to periodic review, it is likely that the EU would insist on more adequate data protection obligations with its African counterparts in the future.

In addition, Kenya has initiated FTA negotiations with the US. Given the strong economic interests that the US has in digital trade, and the provisions included in its past FTAs, it is very likely that this FTA will include provisions prohibiting data localisation requirements.

6. CONCLUSION

Data flows have been central to global economic growth in the past decade. However, paradoxically, in the past five years, there has been a proliferation of data localisation requirements adopted by governments across the world, including those in Africa. However, imposing data localisation requirements to address public policy and economic development objectives is not necessarily the best way to achieve these goals.

Data flow limitations could result in high economic and trade losses for African countries because of inadequate in-country physical infrastructure and know-how to manage data effectively. Regional governments could be best served by adopting risk-based data policies that are underpinned by security, trust, and equal access. Notwithstanding the increase in data flow restrictions in Africa, international and regional trade instruments concluded by these countries could provide avenues to mitigate the inimical effects of these otherwise trade-restrictive measures.

ENDNOTES

1 Institute of International Finance (IIF), 'Data Localization: Cost, Tradeoffs, and Impacts Across the Economy', December 22, 2020, p. 1, https://www.iif.com/Publications/ID/4225/Data-Localization-Costs-Tradeoffs-and-Impacts-Across-the-Economy; McKinsey Global Institute, *Digital Globalization: The New Era of Global Flows*, , March 2016, p. 30, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows.

2 McKinsey Global Institute, *Digital Globalization*, p. 76.

3 United Nations Conference on Trade and Development (UNCTAD), *COVID-19 and Commerce: A Global Review* (New York: United Nations Publications, 2021), pp. 25–26; 37–43.

4 Nigel Cory and Luke Dascoli, 'How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them', (Information Technology and Innovation Foundation, 19 July 2021), p. 1, https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost.

5 Cory and Dascoli, 'How Barriers to Cross-Border Data Flows Are Spreading Globally', p. 3.

6 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation).

7 Cory and Dascoli, 'How Barriers to Cross-Border Data Flows Are Spreading Globally', 3–4; Matthias Bauer, Martina F. Ferracane, and Erik van der Marel, 'Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization', Paper Series: No. 30 — May 2016, p. 17, https://www.cigionline.org/static/documents/gcig_no30web_2.pdf.

8 Cory and Dascoli, 'How Barriers to Cross-Border Data Flows Are Spreading Globally', pp. 3-4; IIF, 'Data Localization: Cost, Tradeoffs, and Impacts Across the Economy', p. 2.

9 GSMA, 'Africa's Data Opportunity? Cross-Border Data Flows and IoT', January 2021, PowerPoint Presentation, slide 25, https://www.gsma.com/publicpolicy/wp-content/uploads/2021/01/Africas-Data-Opportunity-Cross-Border-Data-Flows-and-IoT-Webinar-Slides.pdf.

10 See 'Guidelines for Data and Information Management' and 'Guidelines for ICT Service Provisioning' in NITDA's Guidelines on Nigerian Content Development in Information and Communications Technology.

11 Anupam Chander and Uyên P. Lê, 'Data Nationalism', *Emory Law Journal*, 64 (2015), p. 700.

12 Foreword to Guidelines on Nigerian Content Development in Information and Communications Technology.

13 Department of Communications and Digital Technologies of South Africa, Draft National Policy on Data and Cloud, Government Notice No. 44389 of 1 April 2021.

14 Article 29 of Law No. 007/PR/2015 on the Protection of Personal Data prohibits the transfer of personal data to a country that is not a member of the Economic and Monetary Community of Central Africa (CEMAC) or the Economic Community of Central African States (ECCAS), unless this third state ensures a sufficient level of, inter alia, protection of the privacy.

15 Article 49 of Law No. 2008-12 of 25 January 2008 on the Protection of Personal Data. [check] [Could be: Article 49 of the Protection of Personal Data Act, 2008.]

16 Section 72 of the Protection of Personal Information Act, 2018.

17 Article 51 of the Protection of Personal Data Act, 2013.

18 Section 19 of the Data Protection and Privacy Act, 2019.

19 Section 28 of the Data Protection Act, 2021.

20 Pursuant to Guideline 4.4.8 of the Central Bank of Nigeria's mandatory 2011 Guidelines on Point of Sale (POS) Card Acceptance Services, requires entities engaging in POS card acceptance services in Nigeria to use a local network switch for all domestic POS and Automatic Teller Machine (ATM) transactions. Domestic transactions may not be routed outside Nigeria for switching between Nigerian issuers and acquirers.

21 Pursuant to Section 68 of the National Payment Systems Act of 2020, all electronic money issuers must establish and maintain their primary data centres for payment system services in Uganda.

22 Article 3 of Regulation No. 02/2018 of 24/01/2018 on Cybersecurity (Cybersecurity Regulation) requires all licensed banks to maintain their primary data in Rwanda. Moreover, pursuant to Article 4 of Law No. 16/2010 of 07/05/2010 Governing Credit Information System[s] [sic] in Rwanda, sharing of customer information outside of Rwanda is only permitted with the permission of the Rwandan Central Bank. Additionally, Article15.2(d) of the Regulation No. 03/2018 of 24/01/2018 on Outsourcing, referring to the Cybersecurity Regulation, also prohibits a bank from outsourcing its primary data outside Rwanda.

23 Article 15 of Regulation No. 010/R/CRCSI/RURA/020 of 29/05/2020 governing Cybersecurity prohibits networks, systems and applications of licensed ICT companies from being managed, hosted, remotely accessed or located outside Rwanda, unless explicitly authorised by the Regulatory Authority. Pursuant to Article 36, licensees that contravene the regulations will be subject to financial penalties.

24 Section 18 of the Cyber Security and Cyber Crimes Act of 2021 has an explicit data localisation requirement for 'critical information'.

25 For example, Article 17 of the Ministerial Instructions No. 001/MINICT/2012 of 12/03/2012 related to the Procurement of ICT Goods and Services by Rwanda[n] [sic] Public Institutions provides that all government systems and applications that process, store, and provide critical government data and information must be hosted in the National Data Centre.

26 See NITDA's 'Guidelines for Data and Information Management' and 'Guidelines for ICT Service Provisioning'.

27 CIPESA, 'Mapping and Analysis of Privacy Laws and Policies in Africa', November 2021, p. 48, https://cipesa.org/?wpfb_dl=479. (CIPESA)

28 CIPESA, 'Mapping and Analysis of Privacy Laws and Policies in Africa', p. 34.

29 See Article 48 of Law No. 058/2021 of 13 October 2021 relating to the Protection of Personal Data and Privacy.

30 USTR, 2018 Fact Sheet: Key Barriers to Digital Trade, March 2018, https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2018/march/2018-fact-sheet-key-barriers-digital.

31 USTR, Fact Sheet on 2019 National Trade Estimate: Key Barriers to Digital Trade, March 2019, https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2019/march/fact-sheet-2019-national-trade-estimate.

32 IIF, 'Data Localization', pp. 2–3.

33 Africa Data Centres Association, https://map.datacente.rs/africadatacenters/.

34 Chander and Lê, 'Data Nationalism', p. 722–723.

35 Ibid.

36 Chander and Lê, 'Data Nationalism', p. 724-725.

37 Cory and Dascoli, 'How Barriers to Cross-Border Data Flows Are Spreading Globally', pp. 1, 14-15.

38 Cushman & Wakefield, *Data Centre Risk Index 2016: Informing Global Location Strategies in a Digital World Expanding at a Phenomenal Pace*, p. 4, https://verne-global-lackey.s3.amazonaws.com/uploads%2F2017%2F1%2Fb5e0a0da-5ad2-01b3-1eb8-8f782f22a534%2FC%26W_Data_Centre+Risk_Index_Report_2016.pdf.

39 Cushman & Wakefield, *Data Centre Risk Index 2016*, p. 8.

40 'Amazon Launches Data Centre Operations in South Africa', *Reuters*, April 22, 2020.

41 Jevans Nyabiage, 'African Nations Continue to put Trust in Huawei for Data Management', *South China Morning Post*, June 28, 2021, https://www.scmp.com/news/china/diplomacy/article/3138917/african-nations-continue-put-trust-huawei-datamanagement?module=perpetual_scroll&pgtype=article&campaign=3138917.

42 Matthias Bauer et al., 'The Costs of Data Localisation: A Friendly Fire on Economic Recovery', ECIPE Occasional Paper No. 3/2014, 2014, pp. 6 and 9, https://ecipe.org/publications/dataloc/; Cory and Dascoli, 'How Barriers to Cross-Border Data Flows Are Spreading Globally', p. 2.

43 Mona Farid Badran and Rizwan Tufail, 'Economic Impact of Data Localization in 5 Selected African Countries: An Empirical Study', p. 33, https://pic.strathmore.edu/wp-content/uploads/2019/03/PIC_RANITP_Economic_Impact_of_Data_Localization_in_5_selected_African_Countries.pdf.

44 Badran and Tufail, 'Economic Impact of Data Localization in 5 Selected African Countries', pp. 45-46.

45 Badran and Tufail, 'Economic Impact of Data Localization in 5 Selected African Countries', p. 46.

46 Anri van der Spuy and David Souter, 'COVID-19 and e-commerce', *Research ICT Africa*, March 31, 2021, https://researchictafrica.net/2021/03/31/inside-the-digital-society-covid-19-and-e-commerce/.

47 See IIF, 'Data Localization', pp. 4–8.

48 Ziyang Fan and Anil K. Gupta, 'The Dangers of Digital Protectionism', *Harvard Business Review*, August 30, 2018, https://hbr.org/2018/08/the-dangers-of-digital-protectionism.

49 DLA Piper, Data Protection Laws of the World: Full Handbook, downloaded on 30 September 2021, https://www.dlapiperdataprotection.com/.

50 Three-member panels of individuals adjudicate the first-instance stage in a WTO dispute.

51 Panel Report, *Mexico – Telecoms*, para. 7.28.

52 Daniel Crosby, 'Analysis of Data Localization Measures Under WTO Services Trade Rules and Commitments', March 2016, p. 3, https://e15initiative.org/publications/analysis-of-data-localization-measures-under-wto-services-trade-rules-and-commitments/.

53 Appellate Body Report, *US – Gambling*, para. 239.

54 Panel Report, *US – Gambling*, para. 6.285

55 Appellate Body Report, *China – Publications and Audiovisual Products*, para. 296.

56 WTO Electronic Commerce Negotiations, Updated Consolidated Negotiating Text – September 2021, Revision, INF/ECOM/62/Rev.2, 8 September 2021.

57 Henry Gao, 'Chapter 15: Data Regulation in Trade Agreements: Different Models and Options Ahead', in Maarten Smeets (ed), *WTO Chair Programme: Adapting to the Digital Trade Era: Challenges and Opportunities*, (Geneva WTO, 2021), pp. 331-332.

58 CBPRs, http://cbprs.org/.

59 See Cory and Dascoli, 'How Barriers to Cross-Border Data Flows Are Spreading Globally', p. 22; see also Fan and Gupta, 'The Dangers of Digital Protectionism'.

60 Idris Ademuyiwa and Adedeji Adeniran, 'Assessing Digitalization and Data Governance Issues in Africa', Centre for International Governance Innovation (CIGI), CIGI Papers No. 244 – July 2020, July, 9 2020, https://www.cigionline.org/publications/assessing-digitalization-and-data-governance-issues-africa/.

61 Benin, Chad, Comoros, Congo, Ghana, Guinea-Bissau, Mauritania, Mozambique, Rwanda, Sierra Leone, Sao Tome & Principe, Togo, Tunisia, and Zambia. See https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf.

62 Angola, Ghana, Guinea, Mozambique, Mauritius, Namibia, Rwanda, and Senegal.

63 Article 12 of the ECOWAS Supplementary Act.

64 See European Commission, 'Economic Partnerships', https://ec.europa.eu/trade/policy/countries-and-regions/development/economic-partnerships/.

65 Including the Guidelines on Computerised Personal Data Files (as amended by the United Nations General Assembly on 20 November 1990) and the Recommendation of the OECD Council of 23 September 1980 concerning guidelines governing the protection of privacy and trans-border flows of personal data.

66 At Article 44.

67 Article 56(c)(ii) of the EU–ESA EPA, Article 89(c)(ii) of the EU–Cameroon Interim EPA, and Article 68(c)(ii) of each of the EU–Ghana and EU–Côte d'Ivoire Stepping Stone EPAs. There provisions are similar to the exception under Article XIV of the GATS.

68 Article 10 of the Protocol on Mutual Administrative Assistance in Customs Matters of the EU-SADC and EU-ESA EPAs, the EU–Cameroon Interim EPA, and the EU–Ghana and EU–Côte d'Ivoire Stepping Stone EPAs.

POLICY BRIEF 08

MANDELA INSTITUTE

ABOUT THE MANDELA INSTITUTE

The Mandela Institute is a centre in the School of Law of the University of the Witwatersrand. The Mandela Institute conducts research, develops policy and offers basic and advanced teaching in different areas of law. Further, the Institute conducts executive teaching, training and capacity-building through offering short-course certificate programmes, conferences, and public seminars in areas of law and policy which are domestic in operation but are impacted by global developments.

ABOUT THIS POLICY BRIEF

This Brief is part of a series of publications under the Mandela Institute's 2021 research project on The Economic Impact of Data Localisation in Africa. This project is funded by Facebook.

ABOUT THE AUTHOR

Kholofelo Kugler Kholofelo Kugler is a PhD candidate in Digital Trade at the University of Lucerne, Switzerland. She is also Counsel to the Advisory Centre on WTO, Geneva, Switzerland and a visiting research fellow at the Mandela Institute, Wits University. She holds a Masters degree in International law and Economics from the World Trade Institute, University of Bern.

Mandela Institute, School of Law
School of Law Building
Braamfontein West Campus
University of the Witwatersrand
Johannesburg 2000
South Africa

www.wits.ac.za/mandelainstitute

Design and layout by COMPRESS.dsl | 800607 | www.compressdsl.com