POLICY BRIEF 09

MANDELA INSTITUTE

EXPLORING POLICY TRADE-OFFS FOR DATA LOCALISATION IN SOUTH AFRICA, KENYA AND NIGERIA

Fola Adeleke

MANDELA INSTITUTE, SCHOOL OF LAW,
UNIVERSITY OF THE WITWATERSRAND

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG

CONTENTS

ABSTRACT

The adoption of data protection laws, policies and regulation is increasingly gaining traction in Africa. These legal frameworks, broadly referred to as data protection, adopt different models to regulate cross-border data flows. In South Africa and Kenya, a conditional cross-border transfer model has been adopted while in Nigeria, strict sectoral regulation has been adopted to restrict the international transfer of data. These restrictive transfer models, broadly characterised as data localisation, are justified on several fronts, from data privacy to national security, reflecting the policy priorities of states. While data localisation is difficult to define, this brief adopts the term to describe the prevention of cross-border data flows. While some concerns of African states in relation to unrestricted data flows are valid, they stand at odds with the economic objectives of these countries to use the data economy as the pivot for sustainable economic growth. Using South Africa, Kenya and Nigeria as case studies, this brief reflects on the findings of the country reports and policy briefs produced under the Mandela Institute's research project on data localisation in Africa. The aim is to identify policy trade-offs in the areas of competition, trade and foreign direct investment where data protection approaches need to be reconciled with the unique features of the data economy. To address some policy concerns of states, this concluding brief in our research project recommends that data protection frameworks should adopt a broad expansion of the rights of data subjects to include rights to data portability, access, rectification, fair and reasonable usage, and anonymisation. Furthermore, a cross-harmonisation of laws is necessary and existing regional frameworks such as the Malabo Convention can fulfil a regulatory gap that can safeguard cross-border data flows without restrictive data localisation laws at the country level.

1. INTRODUCTION

Africa's data economy[1] is growing and some African countries are already making a pivotal shift in centring their data economy as the key driver for post COVID-19 pandemic economic recovery.[2] With new technologies shaping the global economy, a progressive approach towards data protection presents an opportunity for states to build economies that can advance economic and social inclusion. However, African countries, hampered by lack of regulatory clarity on data protection, have not fully maximised the opportunities that digital innovation presents. As African states develop regulations to catch up with the pace of digital innovation, there are emerging outcomes that demand our attention. These include understanding the impact of emerging data protection regulation on key economic drivers such as trade, investment facilitation, competition, regional economic integration and economic growth.

Data[3] is driving the industrial revolution that we are witnessing in the 21st century and states are increasingly adopting measures to control and, in some instances, claim ownership of the driving force behind the unfolding technological innovations.[4] Data protection regulation in the three countries of study in this project – South Africa, Kenya and Nigeria – includes the restriction of cross-border flows of data across countries with an impact on data processing. Data localisation is often justified based on five broad objectives: protection of personal data, access to data by local law enforcement, ensuring national security, advancing local economic competitiveness and levelling the regulatory playing field.[5] However, a closer look at these justifications reveals the other unintended consequences of data localisation on free trade, transaction costs and the efficiency of firms, stifling of innovation, and the hampering of economic growth. With global data flows raising global gross domestic product (GDP), it is apposite to ask what policy trade-offs are necessary to balance the legitimate concerns of countries against the unintended consequences that the impact of data localisation causes.

This question is examined through the lens of regional integration and development, with a focus on South Africa, Kenya and Nigeria. The country research reports released earlier in this project addressed the national approaches towards data localisation and various thematic briefs assessed the role of regional and international commitments made by these countries in their various regional blocs and membership of international state bodies.[6] The findings from the earlier work produced in this project show that legal approaches towards data localisation can create challenges for developing countries, and hamper the growth of their economies.[7] While there is an opportunity for international and regional frameworks to play a role and influence developments in member countries, the non-ratification of the African Union (AU) Convention on Cybersecurity and Personal Data Protection in Africa creates a vacuum at the regional level.

In the country research for South Africa, Kenya and Nigeria, we see that Africa's big economies are rolling out various economic policy positions that focus on data protection. The focus on data protection is driven by the idea that as firms expand their products and services into countries, data protection becomes crucial to exercise accountability and to preserve state interests in the development of their data economy. Perceptions of data as the driving commodity for the data economy have been eliciting conceptual problems on the true nature of data and how to regulate it. The conceptual difficulty in understanding data has led to various ideological positions that are spurring state regulatory responses akin to protectionism, state control and ownership of data, revised competition regulation, a shift in priorities for international trade and the attraction of foreign direct investment.

A progressive approach towards data protection presents an opportunity for states to build economies that can advance economic and social inclusion.

This paper captures the emerging issues arising from the country reports and policy papers that have been produced in this research project. In discussing the economics of privacy and the trade-offs arising from data protection enforced by government regulation on the one hand, and private interests in the processing of personal data on the other, we need to understand the economic nature of data, and the value of data, including how value is created and measured. Section 2 of this paper looks at the nature of data and its value and unpacks the findings made by Razzano in her brief titled 'Missteps in the Value of Data'.[8] Section 3 looks at the various country approaches on data localisation from a national and sub-regional perspective, drawing on the country papers produced on South Africa, Kenya and Nigeria. Section 4 builds on the thematic briefs on competition, trade and investment and makes some key findings on the unintended consequences of data localisation in these economic

areas. Section 5 provides some recommendations on how policymakers from African countries that are yet to adopt data protection laws should approach data protection in the future to grow the data economy.

2. THE NATURE OF DATA AND ITS VALUE

To understand the economic implications of data regulation, we first need to know the forms of data that these regulations target. This project primarily focuses on the processing of personal data.[9] This form of data is important for the development of the data economy and the unique characteristics of personal data have led to calls for the government to, for example, 'play a more central role in the collection, dissemination, and analysis of data, understanding that key economic advantages are contained within it'.[10] South Africa's Draft National Policy on Data and Cloud also suggested turning 'digital infrastructure' and data centres, which hold critical cloud computing, into national strategic assets.[11] Such proposals misunderstand the nature of personal data and are often due to the characterisation of data as a form of resource that can fall under state ownership and the supply of which can be regulated.

As a result, we see policy positions such as the need for South Africa 'to derive socio-economic benefits from its data' and for data to be 'a common good for all residing in South Africa'.[12] Analogies such as 'data is the new oil' create the impression that data is finite and constrained to the borders of a country. This has led to the development of policy positions such as South Africa's new position paper seeking to characterise data as a strategic asset for the data economy, to restrict its flow and to impose state ownership of it.[13] This has also led to calls for regulation to break up the monopoly of tech firms, as is the case with oil firms.[14] These positions fail to recognise the key characteristics of data, its generation, storage, flow and how value is generated. This is worth unpacking briefly.

There are four central actors in the generation of value from data. The first is the data subject. Where personal data is involved, the data subject maintains an interest in the processing of the data. The second is the data controller who determines the purpose and means of processing data. The third is the data processor who processes data on behalf of the controller,[15] and the final actor is the regulator, acting on behalf of the state but in most cases with independent powers to monitor and enforce regulatory compliance. All these actors have interests in the outcome of data processing, with the risks – but not necessarily the economic benefits – borne by the data subject. Several factors come into play, including the purpose of processing, the means used to process and the sector where the processed data is applicable. This diversity in outcomes for data value can lead to a fragmented regulatory approach for sector-specific treatments of data processing.

The value of data is dependent on the ability of a processor to use it, which makes the value vastly different from one user to the next. Furthermore, the use of the data determines the value of the data. It should also be noted that not all data is the same. The structured nature of data, the size and aggregated nature of data all play a role in the valuation of data.

The non-rivalrous nature of data makes the idea of data ownership difficult. This means that at a technological level, data is infinitely usable. Due to the non-rivalrous nature of data, access to and control of data is more important than data ownership.[16] Furthermore, the interconnectedness of data linking a subject's data with another makes it difficult to, for example, separate and claim exclusive ownership of personal data. However, data aggregators hold a better claim to data ownership given their ability to process data in a particular form with a specific outcome that serves their interests and in a manner that is de-identified from the original data. An important way to address issues around data ownership is then to unroll a bundle of data subject rights, such as right to portability, access, rectification, fair and reasonable usage and anonymisation. This rights-based approach allows a nuanced understanding of the necessary trade-offs for data use. However, this approach does not address issues around personal vs collective data rights.

> The focus on data protection is driven by the idea that as firms expand their products and services into countries, data protection becomes crucial to exercise accountability.

According to Chapelle and Porciuncula, 'data is not a monolith'.[17] The production process that creates a data value chain ensures that data is not static.[18] This value chain creates different forms of data. The most common distinctions of data relate to personal and non-personal data. However, other forms within this broad distinction exist. These include public vs private data, structured vs unstructured data, open vs proprietary data, anonymised vs pseudonymised data, stored vs real-time data, and human-generated vs machine-produced data.[19] These classifications reflect the nature of the data, degree of

processing, intended use of the data, and the applicable sector generating or using the data.[20] For any of these classifications, the processing determines the ultimate nature of the data and, quite often, the processor and processing determines the value of the data. For example, claims that data is 'the new oil' are inaccurate because oil, unlike data, is a natural resource that is measurable, tangible, limited and strictly regulated.[21] The extent to which processors can extract value from data depends on the purpose of its use.[22]

The value of data is hard to measure and the derivation of value from data should emanate from taxation and not ownership, according to Van der Berg.[23] However, forms of possible taxation are beyond the scope of this research project. It is also important to note that the generation of value can involve complex value chains with different processors having access and processing at a point in time. Therefore, multiple values can be generated based on the extent of processing at a point in time. In addition, restricting the further flow of data may have adverse consequences for processors along the value chain that may restrict the attractiveness of a country for processing. From a trade perspective, data localisation hinders the competitiveness of a country given the lack of comparative advantage in processing data. Therefore, data localisation regulation is a form of protectionism that has the impact of hindering international competition in the data economy.[24]

In addressing the economic consequences of data protection regulations, it is necessary for such regulatory approaches to maintain a level playing field.

An important characteristic of data is that it is an excludable resource. A data controller can restrict access to data through a number of means and security features; however, once data is released publicly, it becomes de facto non-excludable.[25] This is important in understanding the effectiveness of data localisation in certain instances, given the fact that exclusive control over data cannot be guaranteed by a data holder. Furthermore, the location of data can be deliberately left fluid for the purposes of security by replicating the data in several locations through geo-redundancy.[26] This serves the purpose of data protection, which ironically is the same reason some states advocate for the restriction of data in a single location. Aside from the counterproductive effect of localisation, localisation measures also often require expensive technical measures to restrict data to a specific country, which may be beyond the reach of many data processors.

Another reason for data localisation is for national security purposes, including the ability for law enforcement to conduct criminal investigations, for example, or to prevent foreign surveillance. However, there are documented precedents of states using access to data under their jurisdiction for local surveillance on citizens, which is concerning for the rule of law and respect for the right to privacy.[27] In addition, justifications for data localisation, such as for law enforcement purposes, are not necessary in practice. This is due to mandatory requirements for firms to nevertheless comply with government access requests for data regardless of where the data may be stored.

In addressing the economic consequences of data protection regulations, it is necessary for such regulatory approaches to maintain a level playing field, such as through revised competition regulation, trade and investment objectives (discussed later). However, we first need to understand the current data protection trends in the selected countries in relation to the economic objectives identified earlier.

3. DATA PROTECTION APPROACHES IN SELECT AFRICAN COUNTRIES

3.1. South Africa

South Africa's Protection of Personal Information Act provides that a responsible party (data controller or processor) in South Africa may not transfer personal data to a party in a foreign country unless certain requirements are met.[28] These requirements include the data subject's consent, for the recipient of the data to be subject to law, binding corporate rules or a binding agreement that constitutes an adequate level of protection.[29] Alternatively, the data transfer must be a requirement to conclude or perform a contract, or be for the benefit of the data subject and consent cannot reasonably be obtained.

As Van der Berg notes in her country report on South Africa, South Africa's approach is consistent with the European Union's (EU) General Data Protection Regulation (GDPR).[30] However, in a recently published draft policy on data and cloud governance, there is a new attempt by government to control data by requiring data classified as critical information infrastructure to be processed and stored within the borders of South Africa.[31] Furthermore, the policy provides that data generated in South Africa shall be

the property of South Africa, regardless of where the technology company is domiciled.[32]

South Africa's conditional flow of data transfer in the Protection of Personal Information Act is considered 'a balanced and moderate approach …' that is consistent with international law and meets the United Nations High Commissioner for Human Rights necessity criteria, that cross-border data flows are necessary in today's globalised world, and that strict data localisation requirements should be avoided.[33] This position is also consistent with the African Commission on Human and Peoples' Rights (ACHPR) Declaration of Principles on Freedom of Expression and Access to Information in Africa of 2019.[34] Principle 40 of the Declaration provides that 'states shall not adopt laws or other measures prohibiting or weakening encryption, including backdoors, key escrows and data localisation requirements, unless such measures are justifiable and compatible with international human rights law and standards'. As Van der Berg notes,[35] the Declaration reflects the potential of data localisation requirements to jeopardise security and privacy.

3.2. Kenya

In recent times, the GDPR is regarded as the benchmark for data protection regulation globally and this has been the foundational framework for data protection regulation adopted by other countries, including Kenya. However, there have been modifications to the adopted standards. For example, in the Kenya country report produced in this project, Kijirah and Thuo show that Kenya's Data Protection Act (DPA) of 2019 is similar to the GDPR but contains some notable departures.[36] For example, the definition of a 'data processor' under Kenya's DPA includes a 'public authority, agency, or other body'. This is broader than the GDPR's definition and requires public agencies to conduct data protection impact assessments on its own processing.

According to Kijirah and Thuo, the drivers of data localisation in Kenya include revenue collection, national security and cloud computing.[37] They note that the introduction of any restrictive data localisation measures may impede the ability of businesses and individuals to make full use of data, and, in effect, increase the cost of services that require data processing and thus weaken the competitiveness of the market.[38] The Kenyan Competition Authority has published guidelines on data-driven markets for firms in the sector to regulate their conduct and to understand what constitutes anti-competitive conduct.[39] However, the data economy is so unique that traditional competition regulation may not be responsive to the challenges that market dominance creates in the data economy. In situations where products and services are offered without a financial cost to the consumer, competition regulation that aims to, for example, tackle price discrimination is ineffective, as it does not take into account other more important dimensions such as data protection. The challenges with competition regulation in a data economy are discussed in more detail in section 4.

3.3. Nigeria

Nigeria's justification for its data localisation policy in terms of its guidelines for information and communication technology (ICT) is to address a 'negative trade balance' in the ICT sector.[40] In Nigeria's eight-pillar National Digital Economy Policy and Strategy, one of the objectives is to 'harness the capacities of its agencies and properly blend them with the roles of the private sector, in building a flourishing digital economy for the benefit of Nigerians'.[41] However, local data storage solely based on cloud storage does not create jobs or innovation, which are important for a flourishing digital economy, especially since cloud storage systems are managed remotely.

4. POLICY PRIORITIES FOR STATES IN THE DATA ECONOMY

4.1. Competition

There are emerging practices in the data economy that curb the effect of data concentration in a few market players. Such practices include interoperability, which enables cooperation in data usage to mitigate the effect of data concentrations and potentially allow new market entrants.[42] Interoperability is part of a broader set of measures that need to feature in an effective competition regulation that responds to the unique features of the data economy.

There are significant investment costs associated with setting up digital infrastructure and the nature of the data industry allows the dominance of firms.[43] These unique features of the industry include network externalities where the value of usage for all consumers increases as the number of users increases.[44] In addition, the marginal cost of expanding a customer base is minimal, which allows a data processor to control vast amounts of datasets – this can create barriers to entry for small market players.[45] Furthermore, entry barriers such as consumer behaviour, where some firms are preferred over others, also lead to what has been described as 'competition for the market rather than competition in the market'.[46]

In the data economy, data is an input of production[47] and firms with access to tremendous amounts of data can entrench their market position. Processing such large sets of data allows firms to develop and deliver customised services and products that build consumer loyalty.[48] This situation can potentially tempt firms into processing datasets beyond the original purpose of collection to entrench market power. Such practices would violate the purpose limitation principle in data protection regulation as well as competition regulation. Both forms of regulation complement each other as they aim to create an environment that is consumer centric and protects new market entrants.

The nature of personal data-based services is one where many consumer products or services are offered without any financial cost to the user. This makes competition regulation on predatory pricing, which is one of the measures designed to curb abuse of dominance by firms, obsolete. Due to this unique characteristic of data usage, current competition regulation applicable in the majority of African states is not designed to address the economics that drive the data market today.[49]

Aside from the need for regulation that is responsive to the data market, collaborative effort among regulators for monitoring and enforcement of market players who are globally dominant is necessary. It is also important for regulators to bear in mind that a 'one size fits all' approach to regulation that aims to target multinational foreign firms can hinder the ability of smaller data firms to compete in the data market. An example of this would be demands for data localisation when cloud storage across borders may be more cost effective.

Harmonisation of regulation is one way forward in addressing gaps in competition enforcement. The existing regional competition authorities in Africa, such as the Common Market for Eastern and Southern Africa Competition Commission, the Economic Community of West African States Competition Authority and the East African Community Competition Authority, can serve as the basis for integrating competition policy across the continent. In addition, new agreements such as the African Continental Free Trade Area (AfCFTA) could also 'foster harmonisation on competition policy for the data-driven economy through their competition policy protocols'.[50]

However, independent and well-resourced country-level competition regulators are also necessary and, from an African perspective, the South African model articulated in its competition policy on the digital economy is a useful model to follow.[51] It is also important to note that competition regulation requires the complementary support of other data protection laws focusing on data protection, trade and cross-border data flows, for example.

This complexity of competition regulation for the data economy has led countries such as South Africa to develop regulations against abuse of dominance specific to e-commerce, where a firm can be both a seller and buyer of services in the same market where there is an imbalance in the bargaining power between large and small firms.[52]

One way of addressing this is through data interoperability (the ability for different systems to share and use data in a coordinated, timely manner) or data-sharing agreements (when two or more firms agree to merge their data for access by themselves and possibly third parties).[53] This will require recognising data subjects' right to portability, which is recognised in Kenya's data protection law and Nigeria's data protection regulation.

Harmonisation of regulation is one way forward in addressing gaps in competition enforcement.

As Klaaren notes, given the social power and policy influence of the digital economy, perhaps it is worth exploring the idea of data portability as the core issue of an emerging policy domain.[54] In exploring the intersection of competition and privacy, Klaaren argues for a right of data portability along three dimensions. The first involves juristic persons as rights holders where small firms can assert their rights against large firms holding data to improve the dynamics of competition.[55] The second involves a strong individualised data that extends beyond personal data collected directly from data subjects but also includes data generated by firms. The third form allows data subjects to have access and control of their data, including authority to direct a data holder to transfer a subject's data to another authorised third party.

It is also important to note that introducing data-sharing agreements and interoperability as part of any competition frameworks should not result in regulatory overreach that will require firms to share privileged commercial data with competitors. Any competition regulation should also complement data protection laws by ensuring that data-sharing agreements, for example, do not contravene consent requirements for further data processing by data subjects. This will also require loose cooperation between competition regulators and data protection regulators to exercise appropriate oversight.

4.2. Trade, investment and cross-border flows

Data protection laws are important in establishing principles for cross-border data flows, including in determining the level of restrictions to be imposed. According to the 2021 World Bank Development Report, data flows operate on a spectrum of three models: open transfers, which allow the free movement of data; conditional transfers, based on conformity with established regulatory safeguards; and limited transfers, where government approval is needed for cross-border transfers.[56] These transfer models illustrate the approaches to cross-border data flows and do not envisage data localisation, either de jure or de facto, as a possible category that can aid such data flows.

The most well-known example of the open transfer model is the United States, where there are no mandatory conditions for data transfers. This approach presents risks, including lack of a guarantee of any minimum standard for personal data protection.[57] The conditional transfer model is the prevailing approach in most data protection laws and has been popularised by the EU's GDPR. This approach typically restricts data flows to countries that have an adequate level of data protection similar to that of the country of origin of the data.

There are economic impacts to these various models of data transfer. For the open transfer model, while businesses are free of any regulatory burden, the security of the data transfers, without any minimum standards to follow, can create a huge cost in the end if data breaches occur. However, compliance with the other models also increases trade costs for firms. Data transfer restrictions will have a bigger cost burden on smaller firms because of the cost of local data storage.

It has also been suggested that 'the opportunity cost of restricting trade in services may be higher in countries that do not have a large domestic market of their own which will not be the case in larger countries with significant domestic markets, where localisation policies may be adopted to protect domestic infant industries from globally dominant competitors'.[58] This, among other reasons, creates a fair degree of cross-border data flow hesitancy. Such hesitations are driven by claims of, for example, data privacy, national security and access to data by law enforcement.

Regarding data privacy, there is a misplaced assumption that data stored within national borders will be protected from privacy breaches. However, this position, which makes data flow static, makes data a sitting target for cybersecurity threats. According to Meltzer and Lovelock, 'data localisation and data residency requirements lead to poor economic outcomes. Policies that constrain the flow of data across borders directly and negatively affect information access and therefore business growth, the capacity for innovation and productivity gains, and the scope for engaging in international trade'.[59] However, cross-border data flows among countries in Africa may in fact boost the competitiveness of each country in the data economy. To facilitate harmonisation of regional data protection frameworks, the ratification of the 2014 AU Convention on Cybersecurity and Personal Data Protection is necessary. In addition, African states should consider negotiating data-sharing agreements to facilitate cross-border data flows.

Some of the negative effects of restricting cross-border data flows include limiting options for consumers in digital commerce, limiting the ability of firms to process large datasets to improve their products and the creation of trade barriers, which ultimately limit the competitiveness of firms. This shows that restricting cross-border data flows has longer-term costs than benefits that may be gained in the short term.

We also need to acknowledge that developing countries do not have enough leverage to introduce a set of regulatory options for data protection that may alienate foreign investors in the data economy. The relatively small markets of these countries and capacity constraints to enforce regulation mean compliance will be largely dependent on the good faith of firms.

Cross-border data flows among countries in Africa may in fact boost the competitiveness of each country in the data economy.

However, any regulatory approach undertaken by a state must not target foreign firms exclusively in order for such rules to pass international trade rules. States can also use sectoral regulations to develop a more targeted approach for data access and sharing in each sector where data localisation might be particularly relevant. It is also important to note that the development of any regulation should not assume the needs of the sector and development; rather, they should be driven by the expressed needs and hindrances faced by the relevant sectoral firms. Kugler notes in her brief on data localisation and trade flows that the Office of the United States Trade Representative (USTR) has flagged Nigeria and Kenya's data localisation measures as 'discriminating against foreign businesses that distribute their data storage and processing globally' and 'will hamper the

development of Nigeria and Kenya's digital economy, and may undermine data security without providing any meaningful benefit to data privacy'.[60]

Consequently, while countries that adopt an open transfer model may experience higher volumes of trade in digital services, a strong domestic data protection regime can also be positively associated with trade flows in digital services. This gives a positive signal to foreign investors and other states that a country respects the rule of law and the protection of the right to privacy specifically. However, it is important for countries to adopt data protection frameworks that suit their domestic context and not simply transplant regulation from elsewhere. It is also worth noting that any regulation for cross-border data flows only extends to personal data protection and does not include non-personal data in order not to extend undue restrictions for the processing of data.

Focusing on data localisation should not take emphasis away from other important data protection measures, such as limiting the collection, use and processing of the data without consent or beyond the original purpose intended for processing.

At a multilateral level, the General Agreement on Trade in Services (GATS) does not prohibit restrictions on cross-border data flows. However, as noted by Abdulrauf and Abe, mandatory localisation and other limitations on cross-border data flows depending on sectoral commitments could potentially violate GATS' 'non-discrimination' principle.[61] At an African regional level, the AU adopted the Convention on Cybersecurity and Personal Data Protection (Malabo Convention), which is yet to enter into force, but also attempts to regulate data flows.

According to the World Bank, 'cross-border data sharing requires cooperation on standard setting and regulatory harmonisation that lies beyond the scope of trade agreements. International efforts to promote technical standards for data protection and cybersecurity are essential to ensure interoperability and must align with global trade rules on data flows'.[62]

While the three countries under review are signatories to the AfCFTA Agreement, which commits to eliminate all forms of barriers to trade and to promote movement of capital and natural persons, any measure on data localisation in a country serves as a non-tariff barrier to trade in both goods and services.[63]

As Abdulrauf and Abe describe it in their country report on Nigeria, 'the eradication or non-deference to data localisation will foster economic transactions and reduce the "prices of imported goods for consumers and producers using intermediate inputs"'.[64]

5. CONCLUSION

Any data protection regime that safeguards the right to privacy but exacerbates poverty, unemployment and inequality, will miss the mark of building a data economy that is rooted in sustainable development.[65] In developing appropriate data protection frameworks, policies should thus distinguish between different forms of data. Furthermore, focusing on data localisation should not take emphasis away from other important data protection measures, such as limiting the collection, use and processing of the data without consent or beyond the original purpose intended for processing.

The countries under focus in this research are not 'in a position where they can afford to make trade-offs between data localisation and other objectives such as inclusive economic growth or the attraction of foreign direct investment (FDI)'.[66] China is the obvious example of a country that has embraced data localisation arguably as a measure to spur the growth of its domestic firms. The trade-offs China made for this objective cannot be quantified in economic terms given the reported exits of foreign firms from the Chinese markets because of these restrictive measures, without a clear knowledge about the impacts of these exits from the Chinese market. The strength and size of the Chinese market suggests that it can potentially withstand any adverse reactions to its data localisation measures by foreign firms. The same effect will not apply to African economies where the exit of firms may have dire economic impacts.

An important policy recommendation for African states is the approach Van der Berg recommends in her country research paper on data localisation in South Africa. She recommends that data sovereignty should be conceptualised along the lines of stewardship models, with the rights of individuals and entities that produce data placed at the forefront of any such approaches.[67] Furthermore, more emphasis should be placed on skills development, including data analytics, to create and capture value regardless of where data is stored.[68]

The Malabo Convention, which was adopted in 2014, has not had the required number of ratifications needed for it to come into force. As Kijirah and Thuo note in the Kenya report, there are challenges that make ratification

of regional frameworks difficult with different country expectations on how to regulate digital trade.[69] African countries are encouraged to ratify the Malabo Convention and to advocate for the rapid development and adoption of a digital trade protocol under the AfCFTA. In addition, equitable multilateral free trade agreements to ensure the trusted and secure flow of data should be considered.

As Africa's economic leaders, South Africa, Kenya and Nigeria should play leading roles in advocating for interoperability and policy harmonisation in Africa. This approach allows for the maximisation of the benefits of the data economy without the adoption of policies that weaken the economic competitiveness of states.

ENDNOTES

1 As argued by Alex Beyleveld in the introductory paper to this project, the digital economy is conceptually different from the data economy 'which developed later thanks in large part to the rise of the digital economy'. Alex Beyleveld, "Data Protection in Kenya, Nigeria and South Africa in the 2020s and Beyond', Policy Brief 1 (Mandela Institute, 2021), p. 2.

2 The South African government published its Draft National Policy on Data and Cloud in April 2021, stating the advent of 41R presents an opportunity to address the social and economic challenges from the COVID-19 pandemic. 'Invitation to Submit Written Submissions on the Proposed National Data and Cloud Policy', 1 April 2021, https://www.gov.za/sites/default/files/gcis_document/202104/44411gon309.pdf.

3 This project adopts the definition of 'data' as espoused by Beyleveld as 'pieces of information that are electronically collected in bulk with a view to using them – for example, through analysing them systematically in order to make behavioural predictions – for a particular economic (usually commercial) purpose'. Data Protection in Kenya, Nigeria and South Africa', p. 2.

4 'Invitation to Submit Written Submissions'.

5 Ethan Loufield and Shweta Vashisht, 'Data Globalization vs. Data Localisation', 2020, https://www.centerforfinancialinclusion.org/data-globalization-vs-data-localisation; Kholofelo Kugler, 'The Impact of Data Localisation Laws on Trade in Africa', Policy Brief 8 (Mandela Institute, 2021).

6 Malcolm Kijirah and Elaine Wangari Thuo, 'Data Protection and Data Localisation in Kenya: Potential Economic Impact and Effect on Kenya's Commitments in Various Regional Treaty Frameworks' (Mandela Institute, 2021); Shanelle van der Berg, 'Data Protection in South Africa: The Potential Impact of Data Localisation on South Africa's Project of Sustainable Development' (Mandela Institute, 2021); Lukman Adebisi Abdulrauf and Oyeniyi Abe, 'The (Potential) Economic Impact of Data Localisation Policies on Nigeria's Regional Trade Obligations' (Mandela Institute, 2021).

7 In addition, the European Centre for International Political Economy's (ECIPE) report on the impact of data localisation regulation showed that countries will suffer substantial GDP losses if blanket data localisation laws are adopted across all sectors.Erik van der Marel et al 'The Costs of Data Localisation: A Friendly Fire on Economic Recovery', 2014 https://ecipe.org/publications/dataloc/

8 Add full source details for Razzano.

9 As Beyleveld notes, 'the "data" referred to in "data protection" are usually limited to personal data, with the word "protection" generally understood as referring to the safeguarding of this type of data'. Beyleveld, 'Data Protection in Kenya, Nigeria and South Africa', p. 4.

10 'Invitation to Submit Written Submissions', 6.

11 'Invitation to Submit Written Submissions', 17.

12 'Invitation to Submit Written Submissions'.

13 'Invitation to Submit Written Submissions'.

14 In the lead up to the federal elections of the USA in 2020, debates to break up the dominant tech firms – Facebook, Google and Amazon – dominated political and academic debates. See https://www.nytimes.com/2020/10/06/technology/congress-big-tech-monopoly-power.html.

15 Not all data protection regulation distinguishes between data controllers and processors, or uses this term, borrowed from the European Union's General Data Protection Regulation (GDPR).

16 Charles Jones and Christopher Tonetti, 'Nonrivalry and the Economics of Data', *The American Economic Review* 110, no. 9 (2020): 2819–2858, https://doi.org/10.1257/aer.20191330.

17 B. de la Chapelle and L. Porciuncula, 'We Need to Talk about Data' (Internet & Jurisdiction Policy Network, 2021), p. 12, https://www.internetjurisdiction.net/news/aboutdata-report.

18 De la Chapelle and Porciuncula, 'We Need to Talk about Data'.

19 De la Chapelle and Porciuncula, 'We Need to Talk about Data'.

20 De la Chapelle and Porciuncula, 'We Need to Talk about Data'.

21 De la Chapelle and Porciuncula, 'We Need to Talk about Data'.

22 Gabriella Razanno, 'Data Localisation in Kenya, Nigeria and South Africa: Missteps in the Valuing of Data', Policy Brief 6 (Mandela Institute, 2021).

23 Van der Berg, 'Data Protection in South Africa'.

24 Yan Carrière-Swallow and Vikram Haksar, 'The Economics and Implications of Data: An Integrated Perspective', 23 September 2019, https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2019/09/20/The-Economics-andImplications-of-Data-An-Integrated-Perspective-48596.

25 Maria Savona, 'The Value of Data: Towards a Framework to Redistribute It', SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 1 October 2019).

26 De la Chapelle and Porciuncula, 'We Need to Talk about Data'.

27 The United States of America is notorious for surveillance on foreign citizens. Other countries, such as Nigeria, have embraced this trend as well, with the acquisition of surveillance technology to snoop on citizens at will under the guise of national security concerns. See https://giswatch.org/en/country-report/communications-surveillance/nigeria.
28 Protection of Personal Information Act, section 72.
29 Protection of Personal Information Act, section 72.
30 Van der Berg, 'Data Protection in South Africa'.
31 'Invitation to Submit Written Submissions'.
32 'Invitation to Submit Written Submissions'.
33 Van der Berg, 'Data Protection in South Africa', p. 11.
34 See https://www.achpr.org/legalinstruments/detail?id=69.
35 Van der Berg, 'Data Protection in South Africa'.
36 Kijirah and Thuo, 'Data Protection and Data Localisation in Kenya'.
37 Kijirah and Thuo, 'Data Protection and Data Localisation in Kenya'.
38 Kijirah and Thuo, 'Data Protection and Data Localisation in Kenya'.
39 World Bank, 'Data for Better Lives' (World Development Report, 2021), 231.
40 The National Information Technology Development Agency (NITDA) introduced the Nigeria Data Protection Regulation (NDPR) in 2019.
41 Federal Ministry of Communications and Digital Economy, 'National Digital Economy Policy and Strategy (2020–2030),' p. 38–39, https:// www.ncc.gov.ng/docman-main/industry-statistics/policies-reports/883-national-digital-economy-policy-and-strategy/file.
42 Jonathan Klaaren, 'Competition Policy and Data Protection in Africa', Policy Brief 5 (Mandela Institute, 2021).
43 As Van der Berg notes in her report, 'cost efficiencies of cloud computing are undermined by unnecessary duplication of infrastructure and fragmented compliance standards. For example, it can cost as high as $800 million to build a major data centre. However, there are major costs related to data segregation between local and other data'. Van der Berg, 'Data Protection in South Africa', p. 9.
44 Idris Ademuyiwa and Adedeji Adeniran, 'Assessing Digitalization and Data Governance Issues in Africa', CIGI Papers No. 244, July 2020.
45 Ademuyiwa and Adeniran, 'Assessing Digitalization and Data Governance'.
46 Ademuyiwa and Adeniran, 'Assessing Digitalization and Data Governance', page.
47 According to Beyleveld, data 'production' refers to information that is collected and stored. Data has been 'produced' only once it has been collected and stored. Once produced, data becomes a factor of production, that is, as an input for producing something else downstream through processing. Data Protection in Kenya, Nigeria and South Africa', p. 3.
48 Beyleveld, 'Data Protection in Kenya, Nigeria and South Africa'.
49 Gene Kimmelman, 'Synching Antitrust and Regulatory Policies to Boost Competition in the Digital Market', in *Models for Platform Governance* (Waterloo, ON: CIGI, 2019).
50 World Bank, 'Data for Better Lives', 233.
51 In 'Competition Policy and Data Protection in Africa', Klaaren discusses South Africa's Competition Commission Policy released in 2020, titled 'Competition in the Digital Economy'. See http://www.compcom.co.za/wp-content/uploads/2020/09/Competition-in-the-digital-economy_7-September-2020.pdf.
52 Klaaren, 'Competition Policy and Data Protection in Africa'.
53 World Bank, 'Data for Better Lives', 234.
54 Klaaren, 'Competition Policy and Data Protection in Africa'.
55 Klaaren, 'Competition Policy and Data Protection in Africa'.
56 World Bank, 'Data for Better Lives', 239.
57 World Bank, 'Data for Better Lives', 239.
58 World Bank, 'Data for Better Lives', 242.
59 Joshua Meltzer and Peter Lovelock, 'Regulating for a Digital Economy: Understanding the Importance of Cross-Border Data Flows in Asia', Working Paper 113 (Brookings Global Economy and Development, 2018), p. 10.
60 Kugler, 'The Impact of Data Localisation Laws', p. 3. The African Continental Free Trade Agreement expressly requires Member States not to discriminate against each other in adopting rules on data protection.
61 Abdulrauf and Abe, 'The (Potential) Economic Impact'.
62 World Bank, 'Data for Better Lives', 246.
63 Kugler, 'The Impact of Data Localisation Laws'.
64 Abdulrauf and Abe, 'The (Potential) Economic Impact', p. 5.
65 Van der Berg, 'Data Protection in South Africa'.
66 Van der Berg, 'Data Protection in South Africa', p. 11.
67 Van der Berg, 'Data Protection in South Africa'.
68 Van der Berg, 'Data Protection in South Africa'.
69 Kijirah and Thuo, 'Data Protection and Data Localisation in Kenya'.

POLICY BRIEF 09

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

Fola Adeleke obtained his PhD at Wits law school and is an Atlantic Fellow on Social and Economic Equity at the London School of Economics. His research interests are in information rights and corporate accountability..

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 | 400544 | www.compressdsl.com