POLICY BRIEF 07

MANDELA INSTITUTE

# DATA LOCALISATION IN KENYA, NIGERIA AND SOUTH AFRICA:

# REGULATORY FRAMEWORKS, ECONOMIC IMPLICATIONS AND FOREIGN DIRECT INVESTMENT

Alexander Beyleveld

MANDELA INSTITUTE, SCHOOL OF LAW,
UNIVERSITY OF THE WITWATERSRAND

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG

# CONTENTS

# 1. INTRODUCTION

This policy brief forms part of a series of briefs on the potential economic impacts of data protection and localisation in Kenya, Nigeria and South Africa. The topics already covered in this series, as well as those still to be covered, span a range of thematic areas, including the implications of data protection and data localisation measures for cross-border data flows and trade, as well as competition law and policy. Building on the detailed country reports produced earlier in this series on the data protection and localisation measures and policies adopted in Kenya, Nigeria and South Africa,[1] this policy brief adds the issue of foreign direct investment (FDI) to the discussion.

Part 2 briefly describes the data localisation elements of the data regulatory frameworks in Kenya, Nigeria and South Africa.

In the third part, the point made is that current evidence suggests that an ad hoc balancing of costs and benefits will be necessary with respect to specifically defined scenarios across different sectors in Kenya, Nigeria and South Africa. The outcomes of such analyses will then have to be aggregated, with due attention to how localisation requirements will affect firms of different sizes, in order to arrive at an overall assessment of whether particular data localisation requirements are worth implementing on balance. One factor forming part of this analysis is the impact of data localisation requirements on FDI flows, especially when it comes to firms in the data economy.

Part 4 offers some thoughts on what data localisation laws and policies may mean for the facilitation of FDI. This discussion is divided into three parts: first, a typology for understanding FDI in the data economy is sketched; secondly, attention is drawn to certain empirical observations about the digital economy, including in relation to the 'internet intensity' of firms in the broader economy and what this has thus far implied for FDI flows; and, finally, the typology developed is then used to discuss what data localisation may mean for facilitating different types of FDI flows in Kenya, Nigeria and South Africa.[2]

Ultimately, the conclusion reached is that it is too soon to say what data localisation requirements imply for FDI flows in Kenya, Nigeria and South Africa. That said, data localisation requirements, whether otherwise desirable or not, could conceivably still be used as part of strategies to lure FDI to Kenya, Nigeria and South Africa. The success of such strategies will necessarily depend on a multiplicity of factors, including the actual extent of the costs imposed by data localisation requirements, how firms with high internet intensity are taxed, the extent of competition between foreign and local firms and the availability of particular types of skilled labour. Therefore, to the extent that Kenya, Nigeria and South Africa do pursue data localisation policies in order to attract FDI, carefully monitored and agile experimentation will be key.

# 2. DATA LOCALISATION ELEMENTS OF THE DATA REGULATORY FRAMEWORKS IN KENYA, NIGERIA AND SOUTH AFRICA

This part briefly describes the extent to which data localisation requirements currently form part of the Kenyan (section 2.1), Nigerian (section 2.2) and South African (section 2.3) legal and policy landscapes.[3]

## 2.1 Data localisation elements of the Kenyan data regulatory framework

The Kenyan Data Protection Act (KDPA), which came into force on 25 November 2019, is currently the central instrument of the Kenyan data regulatory framework. The KDPA explicitly includes provisions on data localisation, but the extent to which data localisation requirements are actually imposed largely depends on: (i) the type of data at issue; (ii) the manner in which the Data Commissioner carries out their functions; and (iii) the extent to which the Cabinet Secretary for Information, Communication, Technology, Innovation and Youth Affairs (Cabinet Secretary) enacts regulations which mandate data localisation.

Section 48 of the KPDA makes the transfer of personal data to other countries conditional on appropriate safeguards with respect to the security and protection of personal data being in place in the foreign country in question or where the transfer is necessary for a number of enumerated reasons. Section 48 should be read together with section 49, which provides for additional safeguards in the context of 'sensitive' personal data and also empowers the Data Commissioner to: (i) request persons transferring data out of Kenya to demonstrate that it has complied with certain elements of section 48; and (ii) prohibit, suspend or subject a transfer to such conditions as may be determined in order to protect the rights and fundamental freedoms of data subjects. Read together, these sections can be seen as giving the Data Commissioner the power to impose *de facto* data localisation requirements by virtue of setting a high bar when defining what constitutes 'appropriate safeguards with respect to the security and protection of the personal data', but only in respect of *personal* data.4

Additionally, section 50 of the KDPA explicitly enables the Cabinet Secretary to 'prescribe, based on grounds of strategic interests of the state or protection of revenue, certain nature of processing that shall only be effected through a server or a data centre located in Kenya'. It should, of course, be pointed out that the KDPA defines 'processing' broadly, which means that the Cabinet Secretary has the power to impose both *storage* and *processing* localisation requirements through enacting regulations.[5] To this end, the Cabinet Secretary has recently published the Data Protection (General) Regulations (KDPA Draft Regulations) for comment. The KDPA Draft Regulations includes provisions that will, if they are enacted in their current form, have implications for the implementation of sections 48, 49 and 50 of the KDPA.

Section 38 of the KDPA Draft Regulations, for example, provides more specific conditions for when personal data may be transferred out of Kenya. Section 40 additionally clarifies that requirements for cross-border transfer may not allow restrictions on cross-border transfers where the transfer falls under one of the enumerated grounds in section 48, arbitrarily or unjustifiably discriminate against any person, impose a restriction on trade and/or are greater than are required to achieve the objective of the restriction. Section 41 adds clarity with respect to the meaning of appropriate data protection safeguards. If these provisions all come into force, they will significantly temper the ability of sections 48 and 49 of the KDPA to be applied in ways which amount to even *de facto* data localisation measures.

However, this still leaves section 50 of the KPDA and section 25(1) of the KDPA Draft Regulations, which would explicitly impose storage and processing localisation requirements, but only in relation to scenarios where personal data are processed for the purpose of 'actualising a public good', a term which is defined in section 25(2) of the KDPA Draft Regulations by way of an openended list which includes examples of specific instances where local storage and processing are required.

## 2.2 Data localisation elements of the Nigerian data regulatory framework

Nigeria has already had certain specific data localisation regulations in place for some time. For example, the Central Bank of Nigeria imposed a set of mandatory Guidelines on Point of Sale (POS) Card Acceptance Services in 2011, guideline 4.4.8 of which, for example, indicates that '[a]ll domestic transactions including but not limited to POS and ATM transactions in Nigeria must be switched using the services of a local switch and shall not under any circumstance be routed outside Nigeria for switching between Nigerian Issuers and Acquirers'.

Additionally, the National Information Technology Development Agency (NITDA) imposed mandatory Guidelines for Nigerian Content Development in Information and Communication Technology (ICT) in 2013 (2013 NITDA Guidelines), the aims of which include, among others, '[stimulating] and [increasing] the production, sales and consumption of high quality information technology products and services developed by indigenous companies that serve the unique needs of the local and global market'.[6] The 2013 NITDA Guidelines include a number of localisation provisions, including guideline 12.1(4), which requires ICT companies to host all subscriber and consumer data in Nigeria, and guideline 14.2(3), which requires all ministries, departments and agencies (MDAs) of Nigeria's federal government to '[e]nsure that all government data is hosted locally inside the country'.

NITDA also issued the Nigeria Data Protection Regulation (NDPR) in 2019, which 'applies to natural persons residing in Nigeria or residing outside Nigeria who are citizens of Nigeria'.[7] The NDPR does not contain local storage or processing requirements, but it does include provisions on the transfer of data from Nigeria to other jurisdictions. Specifically, regulation 2.11 of the NDPR indicates that personal data transferred to foreign countries are subject to the NDPR and that such transfers fall under the supervision of the Honourable Attorney General of the Federation (HAGF). Regulation 2.11 also indicates that NITDA and the HAGF must undertake an adequate level of protection assessments, which entails consideration of a number of factors enumerated in regulation 2.11. Regulation 2.12 provides for exceptions to the general rule that requires an adequate level of protection determination.

> The contemplated rationales in which data localisation requirements may be rooted are readily apparent from the regulatory frameworks.

A Nigerian Data Protection Bill (NDPB) was also published for comment in 2020. The NDPB contemplates the creation of a Data Protection Commission (DPR), which would presumably render the NDPR nugatory and see the function of personal data protection transferred from the NITDA to the DPR. The DPR, if established, would have similar powers to the Kenyan Data Commissioner.[8] The NDPB does not currently, however, contain a provision enabling a member of the Nigerian government to issue regulations which impose local storage and/or processing requirements as in the case of section 50 of the KDPA. As in the case of the GDPR and the KDPA,

however, the manner in which the provisions of the NDPR and the NDPB (if its current provisions were to become part of an Act) are and will be implemented could amount to *de facto* data localisation requirements, at least in respect of *personal* data, albeit that localisation in these instances might not apply across the board but only to certain jurisdictions.

### 2.3 Data localisation elements of the South African data regulatory framework

The South African Protection of Personal Information Act (POPIA) of 2013 does not contain any rules mandating local storage or processing. As in Kenya and Nigeria, however, the law does contain rules on the transfer of personal information outside of South Africa. Specifically, section 72 of POPIA makes the transfer of personal information conditional on a number of specified requirements. As in the Kenyan and Nigerian cases, some elements could be applied in a manner which constitutes *de facto* data localisation requirements (again, albeit that localisation in such instances might not apply to all jurisdictions), in respect of *personal* data, through the manner in which adequacy of protection rules are implemented. POPIA, however, makes it possible to circumvent any such rules, either through consent or through demonstrating that a specific transfer was for the benefit of the data subject.

More recently, however, the South African Department of Communications and Digital Technologies has published the Draft National Data and Cloud Policy (Draft NDCP) for comment, which in its current form suggests that a number of policy interventions be implemented, including that all data which form part of South Africa's critical information infrastructure shall be processed and stored within the borders of South Africa, that a copy of all personal data transferred out of South Africa must be stored in the country for the purposes of law enforcement and that '[t]o ensure ownership and control':

- Data generated in South Africa shall be the property of South Africa, regardless of where the technology company is domiciled.
- Government shall act as a trustee for all government data generated within the borders of South Africa.
- All research data shall be governed by the Research Big Data Strategy of the Department of Science and Innovation (DSI).
- All data generated from South African natural resources shall be [co-owned] by government and the private sector participant/s whose private funds were used to generate such, and a copy of such data shall be stored in the [High-Performance Computing and Data Processing Centre].
- Ownership and control of personal information and data shall be in line with the POPIA.
- The Department of Trade, Industry and Competition through the Companies and Intellectual Property Commission (CIPC) and the National Intellectual Property Management Office (NIPMO) shall develop a policy framework on data generated from intellectual activities including sharing and use of such data.[9]

It remains to be seen whether and to what extent the Draft NDCP will be converted into a final set of policies and/or laws, but it does provide a sense of the direction the South African government potentially intends to follow in the near future.[10]

## 3. RATIONALES AND THE (POTENTIAL) ECONOMIC IMPACTS OF DATA LOCALISATION REQUIREMENTS

The aim of this part is to examine some of the general economic implications of data localisation requirements given their stated rationales. It does so by situating the concept of data localisation within a theoretical economic framework relating to how data markets are constructed and function (section 3.1), before proceeding to contemplating some of the existing empirical literature on the economic impact of data localisation with a view to teasing out whether generally applicable economic principles are discernible based on current evidence (section 3.2).

### 3.1 The impact of data localisation requirements on data markets

In an earlier policy brief in this series,[11] a general economic theory of data markets was sketched and the notion of data *protection* was then situated within the contours of that theory. Here, the idea is to situate data *localisation* within that same theory. To this end, let us first consider some rationales for data localisation. As Svantesson notes, '[c]ommon motivations for data localisation requirements may include data localisation: 1. in the pursuit of cybersecurity; 2. to limit foreign cyberespionage; 3. to assist law enforcement and national security agencies' access to data; 4. for the purpose of minimising and

investigating cybercrime; 5. for the protection of personal data; 6. to cater for cyber-resilience; 7. to provide geo-political advantages; 8. in order to ensure government access to certain categories of data; and 9. to provide economical competition advantages', adding that '[m]any of these motivations for the introduction of data localisation requirements are related, and indeed overlap'.[12] A number of additional discussions often stem from these rationales, including in relation to the meaning and extent of jurisdiction, issues of so-called data sovereignty and questions of the feasibility of attaining a stated goal through data localisation.

Insofar as Kenya, Nigeria and South Africa are concerned, some of the contemplated rationales in which data localisation requirements may be rooted are readily apparent from the regulatory frameworks discussed above. All three countries, for example, have the protection of personal data in mind. All three countries have also put the issues of assisting law enforcement and national security agencies on the table, as well as the idea of ensuring that government has access to certain categories of data. It further appears that all three countries have their economic goals in mind, but the exact extent to which this is the case is difficult to discern, especially given that data localisation requirements have not yet been fully implemented, if at all.

There are very few general economic principles in relation to data localisation requirements discernible on the basis of current evidence, especially insofar as they relate to Kenya, Nigeria and South Africa.

This likely puts Kenya, Nigeria and South Africa at odds with the general approach taken by the United States (US), which is to oppose virtually all forms of data localisation requirements, usually on the basis that data localisation requirements do not actually further the purported goals for which they are enacted. The European Union (EU) takes a similar approach to personal data protection in Kenya, Nigeria and South Africa in respect of local storage and processing requirements, which the EU generally opposes for similar reasons to the US.

An examination of motivations from across the spectrum discussed above provides helpful insights into what governments are purportedly *trying* to achieve. Essentially, as in the case of data protection, governments are taking measures that would result in the alteration of the economic characteristics of data (whether intentionally or not), which, as noted in the earlier policy brief,[13] are still relatively open to conceptual construction and, as such, are malleable; the conceptual construction of these characteristics, moreover, will affect the supply and demand of data, and, consequently, the price.

## 3.2 Data localisation requirements: Empirical evidence and general economic principles?

Ultimately, there are very few general economic principles in relation to data localisation requirements discernible on the basis of current evidence, especially insofar as they relate to Kenya, Nigeria and South Africa, other than the fact that data localisation requirements will undoubtedly impose costs on firms that they would otherwise not have to face. It is true that attempts have been made to quantify these costs across jurisdictions.[14] That said, methodological approaches tend to be blunt and vary a great deal from study to study against the backdrop of rapidly changing political and economic realities. Moreover, data localisation requirements will affect different economic sectors in different ways and it is not always clear who will bear the additional costs associated with data localisation.

For example, it is not clear which companies will bear the additional costs. Supply chains do not merely consist of one company and consumers. They consist of multiple actors with varying amounts of power. One thing that does appear to be relatively certain is that whatever additional costs do result from data localisation requirements will likely disproportionately affect micro-, small- and medium-sized businesses.[15] Whatever costs are ultimately imposed, however, must be ultimately weighed against any benefits which a certain set of data localisation requirements are used to support, including those that will only be realised in the medium to long term.

Whatever costs are ultimately imposed, however, must be ultimately weighed against any benefits which a certain set of data localisation requirements are used to support.

To sum up what need not be a lengthy discussion for the purposes of this policy brief, current evidence suggests that an ad hoc balancing of costs and benefits will be necessary with respect to specifically defined scenarios across different sectors in Kenya, Nigeria and South Africa. The outcomes of such analyses will then have to

be aggregated, with due attention being paid to how localisation requirements will affect firms of different sizes, in order to arrive at an overall assessment of whether particular data localisation requirements are worth implementing on balance. One factor that forms part of this analysis will be the impact of data localisation requirements on FDI flows, especially when it comes to firms in the data economy.

# 4. THE IMPACTS OF DATA LOCALISATION REQUIREMENTS ON FDI IN THE DATA ECONOMY

This part examines what data localisation laws and policies might mean for the facilitation of FDI. The discussion is divided into three parts: first, a typology for understanding FDI in the data economy is presented (section 4.1); secondly, the notion of the 'internet intensity' of firms is introduced, and its implications for FDI flows discussed (section 4.2); and finally, against the backdrop sketched in section 4.2, what the imposition of data localisation requirements may mean for the facilitation of different types of FDI flows in Kenya, Nigeria and South Africa is then explored (section 4.3).

## 4.1 An FDI typology for the data economy

To state the obvious, not all FDI is the same. Dunning and Lundan describe four main types of FDI: (1) natural resource seeking; (2) market seeking; (3) efficiency seeking; and (4) strategic asset or capability seeking.[16] Natural resource seekers 'are prompted to invest abroad to acquire particular and specific resources of a higher quality at a lower real cost than could be obtained in their home country'.[17] The motivation for this type of FDI 'is to make the investing enterprise more profitable and competitive in the markets it serves (or intends to serve) than it would otherwise be' and '[m]ost, or all, of the output of the affiliates of resource seekers tends to be exported'.[18] As for market seekers, '[t]hese are enterprises that invest in a particular country or region to supply goods or services to markets in these or in adjacent countries'.[19] Simply put, market-seeking investment 'may be undertaken to sustain or protect existing markets, or to exploit or promote new markets'.[20]

As for efficiency seekers, their motivation is 'to rationalise the structure of established resourcebased or market-seeking investment in such a way that the investing company can gain from the common governance of geographically dispersed activities', with benefits essentially amounting to those of the economies of scale and scope and of risk diversification.[21] As Dunning and Lundan clarify, these benefits 'stem from cross-border product or process specialisation, the learning experiences that result from producing in different cultures, and the opportunities for arbitraging cost and price differentials across the exchanges'.[22] The intention of efficiency seekers is 'to take advantage of different factor endowments, cultures, institutional arrangements, demand patterns, economic policies and market structures, by concentrating production in a limited number of locations to supply multiple markets'.[23] As for strategic asset seekers, their aim is 'less to exploit specific cost or marketing advantages over their competitors (although these may sometimes be important) and more to augment the acquiring firm's global portfolio of physical assets and human competences, which they perceive will either sustain or strengthen their ownership-specific advantages or weaken those of their competitors'.[24]

> The main reason for firms to invest abroad in the light of data localisation requirements is to expand into new markets or to maintain their operations in existing ones.

This typology still largely holds in the data economy, but insofar as data localisation requirements are concerned, market seeking is perhaps the most pertinent type of FDI. The main reason for firms to invest abroad in light of data localisation requirements is to expand into new markets or to maintain their operations in existing ones. For example, firms including Apple and Tesla have established data centres in China in order to maintain their presence in the Chinese market.[25] This is particularly pertinent in the context of the internet intensity of firms and what this implies for the extent to which they engage in market-seeking FDI.

## 4.2 Internet intensity and FDI lightness

Casella and Formenti rely on work undertaken by the United Nations Conference on Trade and Development (UNCTAD) in producing a paper which clearly illustrates the differences between the FDI patterns observed among firms depending on their 'internet intensity'.[26] They map UNCTAD's digital framework into a conceptual matrix positioning digital categories on the basis of their internet intensity (the internet intensity matrix), along two dimensions: production and operations, on the one hand, and commercialisation and sales, on the other.[27]

Casella and Formenti explain that '[a]t the top end of the matrix are the purely digital [multinational enterprises (MNEs)], the group of internet platforms and providers of digital solutions, where both operations and sales are digital',[28] whereas '[a]t the lower end of the matrix is the heterogeneous group of non-ICT, nondigital firms, some of which are gradually moving towards digital adoption in operations and sales, as confirmed for example by the growing importance of e-commerce in traditional business'.[29] Finally, there is an intermediate position 'covered by digital MNEs with mixed models (digital content and ecommerce) and the group of ICT MNEs (IT and telecom), whose core business activities combine physical and digital elements'.[30]

Casella and Formenti's map reveals that '[i]n business models [characterised] by higher internet intensity, the weight of foreign assets relative to foreign sales tends to be lower' and, as such, 'MNEs in internet-intensive sectors exhibit a higher FDI lightness ratio'.[31] That is, when '[c]omparing the extreme ends of digital exposure … internet platforms have a share of foreign sales that is more than 2.5 times the share of foreign assets, against roughly the same share for traditional MNEs'.[32] Furthermore, 'digitalization tends to break the operational nexus between foreign sales and foreign assets'.[33] As Casella and Formenti further explain, '[n]ot only do highly digital MNEs tend to realize more foreign sales with less foreign assets, there is in fact no correlation between the two, suggesting that commercial presence in foreign markets has no apparent bearing on international investment choices',[34] noting that '[a]cross internet platforms in the UNCTAD sample, the linear correlation coefficient between the share of foreign sales and foreign assets is close to 0'.[35]

Given that most of the largest MNEs in the world have a high internet intensity, the fact that a *greater* internet intensity equates to a *lighter* FDI footprint serves as important context. What it implies is that the globe's largest firms derive most of their value from sales outside of their 'home' markets, this despite the fact that they do very little investing abroad compared to the largest MNEs of a decade or two ago when MNEs seemingly had to invest much more heavily into foreign markets in order to secure foreign sales. This means that the share of foreign affiliates of the world's largest MNEs situated in developing countries has been falling, while the ratio of unremitted foreign earnings to tangible foreign assets has simultaneously sky-rocketed.[36]

Against this backdrop, it is fairly easy to imagine a justification for data localisation measures from an FDI perspective: if firms heavily reliant on data profit heavily from foreign sales without investing as much as MNEs used to invest in foreign markets, why not use data localisation measures as one way to force the issue? Of course, several important questions arise out of the original question. Chiefly, perhaps, is whether this strategy will actually work. In other words, will data localisation measures actually lead to beneficial changes in FDI flows? If so, under what circumstances? The next section attempts to provide brief preliminary answers to these questions.

## 4.3 Data localisation and the facilitation of FDI in Kenya, Nigeria and South Africa

The Kenyan, Nigerian and South African markets are quite substantial in size. It may thus be tempting to use data localisation requirements as part of a concerted effort to get MNEs which exhibit high levels of internet intensity to invest in Kenya, Nigeria and South Africa in order to expand into these markets or maintain current sales. The extent to which such policies are likely to work, however, remains an open question which will depend on a number of variables and will affect different sectors and types of businesses in different ways. Moreover, the extent to which data localisation requirements may contribute to attracting FDI will depend on a variety of other factors, including the extent of the costs identified in Part 3, the use of tax law and policies to incentivise investment from MNEs (or to raise revenue from them), the extent of competition between MNEs and local firms, as well as the development of the kind of skilled workforces that are capable of thriving in the data economy. However, it is important to note that data localisation does not necessarily equate to local presence, with all its attendant benefits to the local economy. For example, companies may comply with a data localisation requirement by simply paying a local data storage company to host their data in a given country.

The extent to which such policies are likely to work, however, remains an open question which will depend on a number of variables.

Whatever policies are adopted must be carefully thought through in relation to these concerns; they must also allow for flexibility and closely monitored experimentation aimed at continuously gauging whether the benefits of an adopted policy outweigh the costs, especially given that data localisation requirements are a relatively new development as a general proposition, and even more so in the case of Kenya, Nigeria and South Africa. Moreover, as the other policy briefs in this series have (and will) illustrate, there are a large number of other considerations when adopting data localisation requirements that extend beyond attracting FDI which must also be considered and may require trade-offs which policymakers will have to consider very carefully.

## 5. CONCLUDING REMARKS

This policy brief described the data localisation elements of the data regulatory frameworks in Kenya, Nigeria and South Africa; contemplated some of the general economic implications of data localisation measures; and offered preliminary thoughts on what data localisation laws and policies may mean for the facilitation of FDI. In conclusion, it should perhaps be reiterated that data localisation requirements and the effects associated with them are still very much a nascent area of study in Kenya, Nigeria and South Africa. Whatever analysis is currently on offer, including that which has been provided in this policy brief, should thus be treated with circumspection: it is only through practical experimentation (the kind of which has yet to take place) that we will be able to assess to what extent our assumptions hold. As much as we might clamour for definitive answers, many of them simply do not exist yet.

# ENDNOTES

1 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', 2021; Shanelle van der Berg, 'Data Protection in South Africa: The Potential Impact of Data Localisation on South Africa's Project of Sustainable Development', 2021; Lukman Abdulrauf and Oyeniyi Abe, 'The (Potential) Economic Impact of Data Localisation Policies on Nigeria's Regional Trade Obligations', 2021.

2 This issue is also addressed by Fola Adeleke in a subsequent brief in this series.

3 For a more in-depth discussion on data localisation in each of these jurisdictions, see the sources cited in note 1.

4 It is worth acknowledging that legitimate debates could be had as to whether conditional flow provisions in data protection laws should properly be understood as forming part of what we understand as 'data localisation' as a general proposition. The aim here is simply to make the point that conditional flow regimes may in fact result in data localisation to a degree, whether intended or not. This is not to suggest that this kind of de facto data localisation should be understood as being akin to explicit data localisation measures.

5 On the distinction, see Helena Ursic et al., 'Data Localisation Measures and Their Impacts on Data Science', in *Research Handbook in Data Science and Law*, eds. Vanessa Mak, Eric Tjong Tjin Tai, and Anna Berlee (Cheltenham: Edward Elgar, 2018), 324.

6 2013 NITDA Guidelines, guideline 5.2.

7 NDPR, regulation 1.2(b).

8 See further NDPB, section 43.

9 Department of Communications and Digital Technologies, Draft National Policy on Data and Cloud, 28, para. 10.4.

10 This does not, however, mean that the Draft NDCP will be adopted in its current form. It is possible, even probable, that a final policy may look quite different.

11 Alexander Beyleveld, 'Data Protection in Kenya, Nigeria and South Africa', year.

12 Svantesson, 'Data Localisation Trends and Challenges', 14.[this is first mention of this source – full details required]

13 See Beyleveld, 'Data Protection in Kenya, Nigeria and South Africa', 3.

14 See, for example, Matthias Bauer et al., 'The Costs of Data Localisation: Friendly Fire on Economic Recovery', ECIPE Occasional Paper (3/2014), 2014.

15 See generally, for example, Richard D. Taylor, '"Data Localization": The Internet in the Balance', *Telecommunications Policy* 44, no. 8 (2020): 102003.

16 John H. Dunning and Sarianna M. Lundan, *Multinational Enterprises and the Global Economy*, 2nd ed. (Cheltenham: Edward Elgar, 2008), 66–67.

17 Dunning and Lundan, *Multinational Enterprises and the Global Economy*, 67.

18 Dunning and Lundan, *Multinational Enterprises and the Global Economy*, 67.

19 Dunning and Lundan, *Multinational Enterprises and the Global Economy*, 69.

20 Dunning and Lundan, *Multinational Enterprises and the Global Economy*, 70.

21 Dunning and Lundan, *Multinational Enterprises and the Global Economy*, 72.

22 Dunning and Lundan, *Multinational Enterprises and the Global Economy*, 72.

23 Dunning and Lundan, *Multinational Enterprises and the Global Economy*, 72.

24 Dunning and Lundan, *Multinational Enterprises and the Global Economy*, 71–72.

25 See Jack Nicas, Raymond Zhong, and Daisuke Wakabayashi, 'Inside Apple's Compromises in China', *New York Times*, 17 May 2021; Trefor Moss, 'Tesla to Store China Data Locally in New Data Center', *Wall Street Journal*, 26 May 2021.

26 Bruno Casella and Lorenzo Formenti, 'FDI in the Digital Economy: A Shift to Asset-Light International Footprints', *Transnational Corporations* 25, no. 1 (2018): 101–130.

27 Casella and Formenti, 'FDI in the Digital Economy', 111.

28 Casella and Formenti, 'FDI in the Digital Economy', 111.

29 Casella and Formenti, 'FDI in the Digital Economy', 111.

30 Casella and Formenti, 'FDI in the Digital Economy', 111.

31 Casella and Formenti, 'FDI in the Digital Economy', 112.

32 Casella and Formenti, 'FDI in the Digital Economy', 112.

33 Casella and Formenti, 'FDI in the Digital Economy', 112.

34 Casella and Formenti, 'FDI in the Digital Economy', 112.

35 Casella and Formenti, 'FDI in the Digital Economy', 112–113.

36 See Casella and Formenti, 'FDI in the Digital Economy', 114.

POLICY BRIEF 07

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

Alexander Beyleveld is a senior researcher at the Mandela Institute. He holds a PhD in International Economic Law (magna cum laude) 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 | 400553 | www.compressdsl.com