POLICY BRIEF 02

MANDELA INSTITUTE

DATA PROTECTION IN SOUTH AFRICA:

THE POTENTIAL IMPACT OF DATA LOCALISATION ON SOUTH AFRICA'S PROJECT OF SUSTAINABLE DEVELOPMENT

Shanelle van der Berg

MANDELA INSTITUTE, SCHOOL OF LAW,
UNIVERSITY OF THE WITWATERSRAND

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG

CONTENTS

ABSTRACT

Poverty, inequality and unemployment remain rife in South Africa. As the country prepares for the Fourth Industrial Revolution (4IR), it is imperative for South Africa to harness developmental opportunities presented in respect of the emerging African digital economy. In particular, the potential value of free-flowing data as a commodity must be acknowledged and exploited in a manner that is congruent with the country's constitutional and developmental obligations and objectives. Moreover, South Africa is obliged to strike a delicate policy balance between the free flow of data and the privacy rights of its residents, in light of the rights to privacy and access to information guaranteed in the Constitution of the Republic of South Africa, 1996 (Constitution). South Africa also bears various national, regional and international obligations in respect of sustainable development, human rights, and trade. This policy brief accordingly identifies relevant constitutional provisions, legislation, and regional instruments that have a bearing on whether and how government introduces data localisation requirements. The relatively modest requirements stipulated in the Protection of Personal Information Act, 2013 (POPIA) are assessed against data localisation's potential advantages and disadvantages. Arguments that a failure to localise data may lead to 'digital colonialism' are unpacked. Furthermore, states' justification for introducing data localisation requirements, including those related to foreign surveillance; privacy and security; and economic development, are scrutinised. Thereafter, arguments that oppose data localisation or 'data nationalism' are explored, with reference to the unique challenges that confront South Africa's policy makers, including a lack of Information and Communications Technology (ICT) infrastructure and serious power constraints. In particular, the polycentric and sometimes perverse consequences that may result from data localisation are set out, and encompass various phenomena such as the 'Protected Local Provider Problem', the 'Jackpot Problem' and the unintended deleterious impacts on Foreign Direct Investment. Ultimately, an assessment is made as to whether current data localisation requirements strike the correct balance, viewed in the light of South Africa's constitutional obligations, development plans and regional commitments. Where policy gaps are identified, recommendations are made for the adoption of data regulation frameworks at the national and regional levels, that take into account competing obligations on the South African government.

1. INTRODUCTION

Data is a key driver of the global digital economy, while data flows and connectivity are increasingly fuelling the global economy as a whole. The so-called data revolution has resulted in the creation of tremendous wealth and value in a short period of time. Enormous amounts of data are being generated, with global Internet Protocol traffic predicted to reach 150 700 GB per second by 2022.[1] The digital economy, with data as its key driver, has also catalysed tremendous innovation across the world, while almost half of cross-border trade is catalysed by digital connectivity. According to some estimates, the digital economy is equivalent to the gross domestic product (GDP) of a G7 country and is growing at a much faster rate than emerging markets.[2]

However, the advantages of development in the context of the digital economy have not been equitably distributed. Instead, benefits are concentrated in a small number of countries and companies, with the United States (US) and China standing out as leaders in the digital economy. Africa in general, and South Africa in particular, must therefore devise innovative strategies to benefit from the digital economy, and capitalise on the value that data potentially holds. At the same time, South Africa must ensure that its data protection regime is adequate for the protection of human rights, such as the right to privacy.

> Three fundamental rights are squarely implicated in the context of data protection, namely the rights to privacy, access to information, and freedom of expression.

This policy brief sets out the potential impact that the introduction of data localisation measures would have on South Africa's project of sustainable development. Data localisation refers to the collection, processing and storage of data within the borders of the country in which the data was generated, and can be contrasted with the free and unencumbered flow of data across borders.

First, an overview of South Africa's constitutional framework and sustainable development commitments is provided, after which the regulatory and policy framework is set out. Thereafter, the arguments for data localisation are juxtaposed against common arguments that support the free flow of data across borders. The policy brief concludes with an assessment of the potential impact of data localisation requirements on South Africa's project of sustainable development and makes several policy recommendations in this regard.

2. CONSTITUTIONAL FRAMEWORK

The Constitution of the Republic of South Africa, 1996 (Constitution) is the supreme law of South Africa, meaning that any law or conduct inconsistent therewith is invalid, whereas the omission to discharge constitutionally imposed obligations will likewise be unconstitutional.[3] In assessing current and proposed law and policy pertaining to data protection with a focus on data localisation, it will thus be important to evaluate regulatory measures against the standards of the Constitution.

Three fundamental rights are squarely implicated in the context of data protection, namely the rights to privacy, access to information, and freedom of expression (which includes the right to receive and impart information or ideas).[4] Notably, the right to privacy includes the right not to have the privacy of one's communications infringed. This right applies to both state and non-state actors, and may only be limited through the auspices of the Constitution's general limitations clause.[5] Ultimately, data regulation must be capable of striking a delicate balance between the protection of the right to privacy, and the guarantee of a free flow of information as found in the rights of access to information and freedom of expression.

When interpreting the South African Bill of Rights, a court, tribunal or forum must consider international law.[6] Article 17 of the International Covenant on Civil and Political Rights (ICCPR) provides that '[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, or correspondence, nor to unlawful attacks on his honour and reputation'. In respect of cross-border data flows, Article 19 of the ICCPR provides:

> 2. *Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds,* ***regardless of frontiers****, either orally, in writing or in print, in the form of art, or through any other media of his choice.*
>
> 3. *The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:*
>
> *(a) For respect of the rights or reputations of others;*

(b) *For the protection of national security or of public order (ordre public), or of public health or morals. [Emphasis added]*

The ICCPR, therefore, recognises the need for the free flow of information across borders, but simultaneously recognises that proportionate restrictions may be introduced for, *inter alia*, national security purposes.

3. SUSTAINABLE DEVELOPMENT

Realising the value posited by the digital economy will be key in capitalising on the promise of the international sustainable development agenda (Agenda 2030), which is based on the fundamental principle of 'Leave No One Behind' (LNOB).[7] It is thus imperative that South Africa – and the African continent more broadly – positions itself to properly benefit from the value represented by the digital economy and one of its key drivers, namely data. A failure to strike a delicate and flexible balance through policy may have long-term consequences that ultimately lead to South Africa being left behind. With less than a decade to go until the Sustainable Development Goals (SDGs), borne from Agenda 2030, are due to be achieved, a global 'whole society' approach is necessary to ensure that the rapidly evolving digital economy does not exacerbate current patterns of systemic inequality and widespread poverty. Agenda 2030 is predicated on, *inter alia*, the imperative for international cooperation and assistance in order not to replicate the oft-unjust status quo. Whereas many SDGs contain means of implementation as sub-targets, SDG 17 is devoted thereto and is entitled 'Strengthen the means of implementation and revitalize the global partnership for sustainable development'. SDG 17 Targets 17.13 – 17.15 deal with the need for global policy coordination and coherence, which are indispensable in seeking to regulate the digital economy and data in particular. Target 17.15 is of special significance in the data protection context and calls on global stakeholders to '[r]espect each country's policy space and leadership to establish and implement policies for poverty eradication and sustainable development'. The 'right to regulate' must accordingly be acknowledged and respected by international state and non-state actors, including relevant Multi-National Enterprises (MNEs). Furthermore, SDG 17 Targets 17.6 and 17.7 seek to promote global partnerships for sustainable development, which are envisaged to include the transfer of relevant expertise and technology.

SDG 10 is also of relevance, in that it aims to 'reduce inequality within and among countries'. Leveraging multi-stakeholder partnerships and the means of implementation envisaged in the SDGs will be crucial for South Africa to optimally position itself as a regional hub in the digital economy. As one of the world's most unequal countries,[8] South Africa must regulate in a manner that ensures that domestic inequality and poverty are reduced while the country – and continent more broadly – remains vigilant not to be 'left behind' in the global data revolution.

In order to ensure that South Africa and the continent benefit from the digital economy, any developments in the data economy should additionally be guided by

> South Africa must regulate in a manner that ensures that domestic inequality and poverty are reduced.

the regional sustainable development agenda, which is captured in *Agenda 2063: The Africa We Want*[9] (Agenda 2063). Significantly, Agenda 2063 is squarely rooted in Africa's history of colonialism and exploitation, thus recognising in its preamble 'the principle of self-reliance and Africa financing its own development'. This principle is incorporated throughout Agenda 2063, and finds clear expression in Aspiration 1, which aims to achieve 'a prosperous Africa based on inclusive growth and sustainable development'. The African Continental Free Trade Agreement (AfCFTA) will be an important vehicle to realise the vision of Agenda 2063. The AfCFTA aims to build a single continental market for goods and services and significantly increase intra-African trade, while reducing 90% of tariffs on goods and removing other barriers to intra-African trade. Significantly, the AfCFTA does not include a protocol on data flows. It does, however, regard the protection of privacy in the transmission and processing of personal data as a legitimate exception to doing trade.[10]

Domestically, South Africa's National Development Plan (NDP) is largely congruent with the SDGs, and likewise aims to address poverty and inequality while tackling unemployment. In particular, the NDP aims to make high-speed broadband internet universally available at competitive prices. Just like human rights and the SDGs are interrelated and interdependent, the NDP is similarly structured so that effective policy action in one sphere may yield positive outcomes for other development goals. For example, the creation of ICT hubs could lead to positive spatial transformation and local inclusive growth for Small and Medium Enterprises (SMEs).

The South African policy environment is therefore embedded in the rich normative framework posited by various sustainable development agendas and frameworks. Any policy measures must promote sustainable

development and inclusive growth while simultaneously guaranteeing an adequate level of data protection in terms of domestic and international human rights standards.

4. THE POLICY AND REGULATORY LANDSCAPE

The Protection of Personal Information Act No. 4 of 2013 (POPIA) constitutes the primary legislation in South Africa aimed at the protection of the constitutional right to privacy. The Act prescribes eight conditions for the lawful processing of personal data,[11] namely 'accountability', 'processing limitation', 'purpose specification', 'further processing limitation', 'information quality', 'openness', 'security safeguards' and 'data subject participation'.[12] The Act further provides for the rights and remedies of data subjects, and empowers the Information Regulator to enforce the Act. Exclusions of certain types of information align with the European Union (EU) General Data Protection Regulation (GDPR).[13] One of the purposes of the POPIA, as set out in the Act's long title, is to 'regulate the flow of personal information across borders of the Republic'. The POPIA sets out modest requirements for the cross-border flows of information in section 72, thereby constituting a conditional flow regime. Personal data may not be transferred by a responsible party in South Africa to a party in a foreign country unless certain requirements are met, for example, that the foreign party is subject to law, binding corporate rules or a binding agreement that constitutes an adequate level of protection; that the data subject consents thereto; or that the transfer is required to conclude or perform a contract, or is for the benefit of the data subject and consent cannot reasonably be obtained. In addition, section 34 of the POPIA prohibits the processing of information of children, unless the processing is done according to the stipulations of section 35. The Information Regulator (the statutory body created in terms of the POPIA) may authorise the processing of personal information of children.

It is noteworthy that, unlike the EU's GDPR, the POPIA only applies to responsible parties that are domiciled within the Republic of South Africa, or who are not domiciled in South Africa 'but makes use of automated or non-automated means in the Republic'.[14] However, the Act's regulation of cross-border data flows is largely congruent with the requirements of the GDPR. Unlike the GDPR, section 72 of the POPIA does not make explicit reference to the receiving jurisdiction observing the rule of law, human rights and fundamental freedoms. Nevertheless, the POPIA is ultimately subject to the Constitution as the supreme law, and the Act aims to give effect to the constitutional right to privacy. According to Snail ka Mtuze, a proper interpretation of section 72 is one that recognises the protection of human rights whenever data is transferred for processing abroad.[15]

> Any policy measures must promote sustainable development and inclusive growth while simultaneously guaranteeing an adequate level of data protection.

At the domestic policy level, the draft National Data and Cloud Policy was published for public comment on 1 April 2021, in terms of section 3(5) of the Electronic Communications Act No. 36 of 2005. The draft policy aims to strengthen the capacity of the state to provide services and develop policies based on data analytics. More broadly, the policy aims to ensure that South Africans benefit from the potential socio-economic value of data by aligning existing laws, policies and regulations, and by creating an enabling regulatory framework in which the data ecosystem can thrive. Although the policy contains noble ambitions for building an inclusive data economy in line with South Africa's sustainable development commitments, the policy is uncosted and it remains to be seen whether it is practically implementable. Furthermore, in its current guise, the policy contains certain vague and sometimes incorrect references to data-related concepts and terminology. This has prompted severe criticism from commentators, who view the policy as a misguided attempt by government to control data in such a way that the right to privacy will be violated while competition in the cloud sphere will be strangled.[16] In its current form, the draft policy is irreconcilable with the regulatory regime constituted by the POPIA.

In respect of data localisation requirements, the policy envisages the following policy interventions:

10.4.1 All data classified/identified as Critical Information Infrastructure shall be processed and stored within the borders of South Africa.

10.4.2 Cross-border transfer of citizen data shall only be carried out in adherence with South African privacy protection policies and legislation (POPIA), the provisions of the Constitution, and in compliance with international best practice.

10.4.3 Notwithstanding the policy intervention above, a copy of such data must be stored in South Africa for the purposes of law enforcement.

10.4.4 To 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] HPCDPC.*
- *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.*

These proposed policy interventions point to a state-centric approach to the data economy. For example, the requirement to store a copy of data within South Africa's borders for law enforcement purposes reflects the Russian approach to data localisation.[17] Of most concern are the statements made regarding the 'ownership' of data and data as 'property'. Clarification is needed in relation to the various statements made in this regard in paragraph 10.4.4 of the draft policy. In addition, the revised policy should take into account submissions from various key stakeholders, including from relevant state-owned entities and the private sector. A regulatory sandbox to test the full extent and meaning of the proposed policy would be exceptionally useful in this rapidly evolving context.[18]

At a regional policy level, the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), which was adopted in 2014, remains inoperative with only eight of the required 15 ratifications secured. South Africa has not yet signed or ratified the Convention.[19] Article 14(6) of the Convention introduces limited data localisation requirements in that personal information may not be transferred to a non-member state unless an adequate level of protection of privacy and other rights is present.

The African Commission on Human and Peoples' Rights (ACHPR) adopted the updated Declaration of Principles of Freedom of Expression and Access to Information in Africa in 2019. The Declaration includes principles regarding freedom of expression and access to information on the internet. Principle 40, which deals with privacy and protection of personal information, holds 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'. The Declaration thus reflects the potential of data localisation requirements to jeopardise security and privacy.

The Support for the Harmonisation of the ICT Policies in Sub-Saharan Africa project (HIPSSA) considers regional texts in sub-Saharan Africa as non-binding measures. The SADC Model Act on Data Protection of 2013 differs slightly in certain of its formulations to those contained in the Malabo Convention. Despite certain differences, Greenleaf and Cottier argue that binding and non-binding African regional initiatives are largely consistent, and that a high degree of data protection harmonisation could be achieved if these instruments formed the basis of national laws or amendments.[20]

These proposed policy interventions point to a statecentric approach to the data economy.

At the international policy level, efforts continue to reach broad international consensus on a fair, universal and interoperable regulatory framework to govern the datasphere.[21] While these endeavours are ongoing, the Organisation for Economic Co-operation and Development (OECD) has been focused on addressing the taxation challenges presented by the rapid digitalisation of the economy, and the move away from a traditional brick-and-mortar model of business. The OECD's work comprises of two pillars, namely 'Pillar One – the re-allocation of taxing rights' and 'Pillar Two – global anti-base erosion mechanism'. The first pillar addresses novel tax issues related to the taxation of corporations that do not have a physical presence in the host country; where and on what basis taxes should be paid; and what portion of profits should be taxed in a jurisdiction where customers or users are located. The second pillar aims to stop the shifting of profits to tax havens; to ensure that MNEs pay a minimum threshold of tax; and to level the playing field between traditional and digital corporations. The work has been ongoing since 2015.[22]

There are various other relevant laws and policies dealing with issues related to data localisation, such as trade and competition, which fall outside the scope of this policy brief. It is nevertheless important to remain cognisant of the far-reaching impacts that the regulation of the free flow of data can have on these and other interrelated spheres, viewed within the broad sustainable development milieu.

5. A POLARISED DEBATE

Current debates on data localisation are polarised as between those who advocate for data localisation – and data sovereignty – and those who advocate for the free flow of data across sectors and borders.[23] There are emerging calls to move away from this polarised position, and to recognise that a dichotomous approach is not necessary or appropriate.[24] Below, arguments for the two primary camps around the issue of data localisation are set out. However, in the final analysis, a delicate and flexible policy balance should be struck to ensure that states' legitimate human rights-congruent concerns are addressed while simultaneously capacitating South Africa to benefit from the value that can potentially be derived from the data-driven economy.

5.1 The case for data localisation

Proponents of data localisation usually advance a combination of economic and non-economic arguments to justify the placing of restrictions on the free flow of information across borders. These arguments should be understood in the context of the evolving global political economy, according to which power and information asymmetries remain vast between developed and developing countries, as well as between MNEs and developing countries. The disproportionate concentration of power and information is compounded by a 'winner-takes-most' economics whereby the rise of 'superstar firms' on the basis of economies of scale and scope, network effects, and information imbalances, may lead to market distortions.[25]

Early analogies that espoused data as the 'new oil' served to spark fears in the Global South that developing countries would again be excluded from economic development in the context of the digital economy. Of course, those analogies are false, and data constitutes a very different commodity that requires *sui generis* regulation to ensure a fair distribution of its potential socio-economic benefits.[26] Socio-economic arguments from nation states have often been met with scepticism by stakeholders who perceive these justifications as merely a guise for increased surveillance of citizens.[27] One thing is certain in this opaque landscape: there is an urgent need for transparency and clarity when thinking about the opportunities and pitfalls of restricting the free flow of data.

Non-economic justifications proffered for data localisation include security and access by law enforcement on the one hand, and the protection of citizens' right to privacy on the other. The staving off of foreign surveillance ostensibly responds to both security and privacy concerns. According to this logic, measures must be adopted to prevent foreign governments from spying on local citizens and businesses. This argument for the introduction of data localisation requirements gained traction in the wake of the Snowden revelations starting in 2013 when it was revealed that the US National Security Agency had maintained surveillance operations that, amongst others, intercepted communications from over 50 000 computer systems worldwide. At the time, BRICS countries reacted by announcing plans to build a network of internet cables that would exclude the possibility of 'eavesdropping' by the US.[28]

The protection of the security and privacy of local personal data is another reason proffered by advocates of data localisation to justify placing restrictions on the free flow of information. Interestingly, countries with weak cyber security protections are often the most vocal in advocating for data localisation measures. This includes Indonesia, Vietnam and Brazil, who have all been exposed to egregious cyber attacks in the past.[29] South Africa has also witnessed various cyber attacks in recent years.[30]

> Socio-economic justifications for data localisation include promoting innovation and inclusive growth at the domestic level through the development of the digital economy.

Socio-economic justifications for data localisation include promoting innovation and inclusive growth at the domestic level through the development of the digital economy, job creation and attraction of capital flows, as well as making evidence-based policy decisions to enrich government services to its people.

The socio-economic arguments advanced for data localisation often overlap with a normative discourse that warns that 'digital colonialism' may exclude developing countries in the Global South from positioning

themselves to fairly derive advantages from the digital economy and the data revolution. Kwet states in this regard:

> *Similar to the technical architecture of classic colonialism, digital colonialism is rooted in the design of the tech ecosystem for the purposes of profit and plunder. If the railways and maritime trade routes were the 'open veins' of the Global South back then, today, digital infrastructure takes on the same role: Big Tech corporations use proprietary software, corporate clouds, and centralised Internet services to spy on users, process their data, and spit back manufactured services to subjects of their data fiefdoms.*[31]

The uneven distribution of power and wealth is apparent when one considers that the value presented by digital 'superstar firms' often dwarfs the GDP of countries such as South Africa. Additionally, global power dynamics can be discerned from the skewed location of data centres, which is concentrated around Europe and the US coastline.[32]

These sentiments are shared by other commentators who caution that the monopoly exerted by digital giants who dominate the data-driven economy is fundamentally anti-development. According to this argument, data as an intangible input to the digital economy differs drastically from previous tangible inputs such as oil. As a result, governments are ill-equipped to regulate amorphous social relations that cannot be anchored in physical space. According to Banga and Kozul-Wright, '[t]his has given rise to a world of disembodied networks and diminished bargaining power of those producing the input'.[33] The authors go on to point out that predatory behaviours by digital superstar firms result in a vicious cycle whereby the exercise of monopolistic power leads to the accumulation of economic power, which allows super firms to capture political power and thus entrench their economic advantage. They conclude that going forward, governments' right to regulate should be guarded, domestic platforms should receive targeted support, and states should continue to encourage technology transfers.[34]

Given Africa's legacy of colonialism and exploitation, socio-economic arguments that call for the decentralisation of wealth and power lest Africa is once again 'left behind' in the development process, are valid. Moreover, care should be taken not to simply equate data localisation measures with protectionism – certain measures that support data nationalism ultimately have a legitimate basis, such as genuine efforts to protect the right to privacy or derive a fair share of socio-economic benefits.[35]

As further explained below, a regulatory balance needs to be struck so that South Africa may capitalise from the benefits of the data revolution and protect fundamental rights, while taking care not to cause unintended and perverse consequences such as increased surveillance, disinvestment or rendering local firms more vulnerable to cyber attacks.

5.2 The case for free data flows

Advocates for the free flow of data do not eschew the *objectives* pursued by states in adopting data localisation measures, as discussed above. Instead, they regard data localisation measures as a blunt tool with which to achieve these laudable goals, and furthermore point out that data localisation measures can often result in unintended and perverse consequences. Below, common counter-arguments to data localisation justifications are set out. It is once again important to bear in mind that a dichotomous, either/or approach will not lead to the equitable distribution of the benefits of the data-driven economy or the sufficient protection of fundamental rights. Instead, a policy balance should be achieved.

The uneven distribution of power and wealth is apparent when one considers that the value presented by digital 'superstar firms' often dwarfs the GDP of countries such as South Africa.

Generally, proponents of the free flow of data point to the architecture of the internet as borderless and open, and the volumes of data generated and transferred, to argue that strong data localisation measures are simply not feasible in the data ecosystem. The non-geographical architecture of the internet and the lack of physical nexus constitute unfamiliar terrain for countries anxious to assert their data sovereignty and not be 'left behind' in the data revolution. The nature of the data at issue, and how it is classified, are also relevant. Thus, for example, in addition to distinguishing between personal and public data, it is also necessary to distinguish between stored versus real-time data and data treated on the edge (such as data inside an automated device or vehicle).[36]

In respect of the non-economic arguments that are usually advanced by states for localisation requirements, those against restrictions on data flows point to the unintended consequences that might result from the imposition of localisation measures. In particular, commentators note that centralising data and

information makes it easier for both hackers and foreign governments to access such data. The 'Protected Local Provider Problem' thus occurs when local firms – who do not need to participate in fierce international competition due to domestic data localisation protections – have fewer resources at their disposal to offer the best and most up-to-date security solutions. The concentration of data also hampers the practice of 'sharding', whereby rows of a database are stored in separate servers across the world so that the data 'shards' are adequate for operations but cannot lead to the re-identification of individuals.[37] Similarly, the 'Jackpot Problem' refers to the fact that the concentration of information in one location may make it easier for foreign governments to exercise surveillance over another nation's citizens.[38] Chander and Lê opine that, ultimately, the only way to avoid foreign surveillance by the US National Security Agency is to not be connected to the internet.[39]

Based on prevailing literature, little attention is granted in these counter-arguments to states' valid concerns and obligations to safeguard the fundamental right to privacy while balancing it with other rights guarantees that require the unencumbered flow of information.

> Data's value is maximized when it can flow with trust and permission across companies, sectors, and national borders to be used.

In respect of socio-economic arguments against data localisation measures, it is notable that most commentators focus exclusively on purely economic consequences while paying insufficient attention to the pressing need for governments to make evidence-based decisions in order to improve social and welfare spending and the delivery of public services to its citizens. The oft-cited (and somewhat controversial)[40] report by the European Centre for International Political Economy (ECIPE) sets out to quantify the economic losses of data localisation requirements and other data protection and security laws that discriminate against foreign data suppliers, and downstream goods and service suppliers. The research shows substantial losses in GDP for all countries that formed part of the study,[41] and projects even greater losses if these countries were to adopt blanket data localisation laws that apply across all sectors. Further findings note impacts on domestic investments for all countries, while exports would decline for China and Indonesia. 'Welfare losses', defined as the actual economic losses of citizens, are projected as approximately US$63 billion for China and US$193 billion for India, with average loss per worker estimated as 11% of average monthly salaries in India, 13% in China and 20% in Brazil and Korea. The authors note the importance of access to foreign markets and global supply chains to promote economic growth and job creation, and further underscore the fact that the manufacturing and export sectors rely on a wide range of services that in turn depend on access to efficient data. The authors conclude:

> *The findings show that the negative impact of disrupting cross-border data flows should not be ignored. The globalised economy has made unilateral trade restrictions a counterproductive strategy that puts the country at a relative loss to others, with no possibilities to mitigate the negative impact in the long run. Forced localisation is often the product of poor or one-sided economic analysis, with the surreptitious objective of keeping foreign competitors out. Any gains stemming from data localisation are too small to outweigh losses in terms of welfare and output in the general economy.*[42]

According to the Institute of International Finance (IIF), the objectives of data localisation measures, such as security, privacy and inclusive sustainable economic growth, are indeed worthy of pursuit. However, the IIF argues that using data localisation measures to achieve these goals displays a misconception of when and how data produces value, and further fails to identify and candidly grapple with trade-offs that need to be made in this context:

> *Proponents of data localization talk about retaining the value of their citizens' data and creating economic opportunity; however, the measures put in place reflect a misunderstanding of what makes data valuable and who ultimately bears the cost of localization requirements.*

Data's value is maximized when it can flow with trust and permission across companies, sectors, and national borders to be used. That trusted and permissioned flow, with economic and legal frameworks to ensure safety, security, and equal access to opportunity, should be the goal of data policy.[43]

The IIF goes on to expound the various costs of data localisation after noting that such costs are borne out by entire economies – both in terms of direct costs and in terms of reduced system efficiencies, reduced access to global value chains, and fewer opportunities to leverage global data and technology resources. According to the IIF, the first cost of data localisation is that it undermines trade and economic growth. The

authors note in this regard that e-commerce (a fast-growing sector that constitutes a subset of cross-border trade as well as domestic retail) is based on the free flow of data, and relies on real-time data connectivity across the economy. The IIF identifies the second cost attendant to data localisation as slowing the digital ecosystem. The authors observe in this respect that instant payment services as well as the operation of fintech could be hampered by data localisation requirements. Furthermore, they note that data localisation can lead to the fragmentation of the internet, which would have significant impacts on various spheres including digital transformation and trade. The IIF identifies a third cost as undermining fraud prevention and cyber security best practices. Finally, the IIF argues that data localisation can block the advantages of cloud computing, noting that data localisation 'could choke innovation' since many start-ups rely on cloud computing to launch. Costs of data localisation are largely transferred to start-ups, Small and Medium Enterprises (SMEs) and consumers, with some estimates showing increased costs for computing needs of up to 60% for local companies who cannot make use of cheaper services located outside of a country's borders.[44] In addition, the IIF notes cost and feasibility concerns in relation to the building of local data centres:

> *Cost efficiencies of cloud computing are undermined by unnecessary duplication of infrastructure and fragmented compliance standards. The cost of data center construction is expensive, with Mastercard reported to spend $350 million to build a new data center in India. For larger data operators such as Amazon, the cost of a tier one data center is in the range of $800 million. However, there are two other major costs. One is the cost to transition, which involves more than a rebuild. First, local data must be separated out from the global data set, and two separate systems engineered. There is also a cost of re-integration of two datasets for anti-fraud monitoring.*[45]

Moreover, the benefits of building local data centre capacity in terms of, for example, job creation, are outweighed by the costs and energy-intensive nature of such endeavours. For data protection to contribute to sustainable development, all elements of the value chain should be sustainable. The unnecessary storage of duplicates will thus have an ecological impact in addition to signalling extra economic costs.[46]

6. ASSESSING THE POTENTIAL IMPACT OF DATA LOCALISATION REQUIREMENTS ON SOUTH AFRICA'S PROJECT OF SUSTAINABLE DEVELOPMENT

6.1 Realising the right to development in pursuit of a thriving digital economy

For the digital economy to contribute to South Africa's project of sustainable development, it must facilitate economic development in tandem with the protection of all human rights guaranteed domestically, regionally and internationally. The Banjul Charter's guarantees of self-determination[47] and for benefiting from development processes are thus relevant. Article 22 of the Banjul Charter recognises the right to development:

> *Article 22*
>
> 1. *All peoples shall have the right to their economic, social and cultural development with due regard to their freedom and identity and in the equal enjoyment of the common heritage of mankind.*
>
> 2. *States shall have the duty, individually or collectively, to ensure the exercise of the right to development.*

Although the South African Constitution does not recognise the 'right to development' as such, South Africa is bound by the provisions of the Banjul Charter and must thus ensure the exercise of this right. The right to development includes a right to the *process* of development, while recognising the duty of states to cooperate to realise this right. The duty of cooperation is recognised both in Article 22(2) of the Banjul Charter, and in SDG 17 of Agenda 2030. The realisation of the right to development would lead to the expansion of the capabilities and freedoms necessary for people to lead valuable and dignified lives. The right to development can be conceived of as a 'vector', as first conceptualised by Sengupta:

> *The right to development as a right to a particular process of development can best be described as a 'vector' of all the different rights and freedoms. Each element of the vector is a human right just as the vector itself is a human right. They will all have to be implemented, in full accordance with*

human rights standards. Furthermore, all the elements are interdependent, both at any point in time and over a period of time, in the sense that the realization of one right – for example the right to health – depends on the level of realization of other rights, such as the rights to food, to housing, to liberty and security of the person or freedom of information, both at the present time and in the future. Similarly, realization of all these rights in a sustainable manner would depend upon the growth of GDP and other resources, which in turn would depend upon the realization of the rights to health and education, as well as to freedom of information given the initial stock of human, material and institutional assets.[48]

The interrelated and interdependent nature of the rights making up the content of the right to development means that the rights to privacy and freedom of information must be guarded and realised while pursuing economic opportunities. Should economic benefits be realised while fundamental rights are violated, any 'development' will not be 'sustainable' as per Agenda 2030, and will likewise not constitute the exercise of the 'right to development' as mandated by the Banjul Charter. The inverse is also true, in that a data protection regime that safeguards the right to privacy but exacerbates poverty, unemployment and inequality, will similarly miss the mark of constituting sustainable development.

6.2 Harnessing the benefits of the data revolution

The potential benefits of the digital economy are vast. Depending on how the 'digital economy' is defined, it can account for up to 15.5% of the world's GDP.[49] Data holds the potential to drive South Africa's sustainable development commitments by providing the information necessary to develop policies and programmes that bring about meaningful socio-economic change. Furthermore, the data economy can spur economic growth, increase employment opportunities and spark innovation.[50]

Data, as a non-rivalrous, non-finite and partially excludable commodity, is very different from traditional commodities such as oil. It cannot be exhausted, and is only partially excludable when restrictions are placed on accessibility. Data is essential for various new technologies, including all internet-based services, the Internet of Things, data analytics, AI and blockchain technologies. Data can also benefit traditional sectors. According to the United Nations Conference on Trade and Development (UNCTAD), 'in virtually every value chain, the ability to collect, store, analyse and transform data brings added power and competitive advantages'.[51]

In the light of the ubiquitous nature of data as a key driver of the digital economy, it is crucial that South Africa finds innovative approaches with which to derive equitable benefits from the data economy. The alternative is for South Africa to be 'left behind', in conflict with the fundamental principle of LNOB that underlies the sustainable development agenda. However, this means that government and stakeholders will need to make a frank assessment of South Africa's current infrastructure and skills capability in order to ensure that it positions itself so as to realistically leverage its regional and BRICS status. The digital divide stretches beyond just internet penetration rates, and also manifests as the grossly skewed geographic location of data centres, with Africa and Latin America accounting for a mere 5% of data centres.[52] Furthermore, data in itself does not have value. It must be used and transformed for value to be created.[53] Even where data is used to promote sustainable development outcomes, there are no guarantees that any value created will be distributed equitably.

According to the UNCTAD:

Local firms in developing countries can benefit from being able to use services offered by global platforms … [L]ocal knowledge (for instance, of search habits, traffic conditions and cultural nuances) may … give an advantage to locally rooted digital platforms, enabling them to offer services tailored to local users. Yet, due to … competition dynamics … developing-country platforms that are trying to scale typically face an uphill battle. The dominance of global digital platforms, their control of data, as well as their capacity to create and capture the ensuing value, tend to further accentuate concentration and consolidation rather than reduce inequalities between and within countries.[54]

As further noted by UNCTAD, the global character of the digital economy means that although national and regional policies are necessary, they are not in themselves sufficient.[55] Instead, international dialogue and consensus-building are required in line with the international cooperation targets set out in SDG 17.

6.3 From polarisation to cooperation

Stakeholders in South Africa should move away from a dichotomous approach to the data localisation debate, and instead, collaborate to find common ground. Before arguments for and against data localisation requirements are assessed, both state and non-state actors should take care to establish clear terms of reference. In the first instance, it is necessary to be clear about the fact that data, in itself, is valueless. Only through data analytics and other manipulations is socio-economic value

created, added and captured. At the same time, data as a non-rivalrous and non-finite commodity, can be infinitely re-used and exploited at low marginal costs.[56]

Second, care must be taken to identify and accurately classify different types of data. Policies should thus distinguish between non-personal and personal data, between sensitive and non-sensitive data, public or private data, stored or real-time data, open or proprietary data, and so forth.[57] Related hereto, the function of data should be correctly understood. References in the draft National Data and Cloud policy that refer to data as the 'infrastructure' of the digital economy should accordingly be rectified.[58]

Third, excessive focus on where data is stored detracts from equally important issues, such as who processes the data, from whom the data is collected and for what purpose. Storage of data is complex, and analogies with traditional concepts such as factories where data is processed, are inapposite. Data can be stored in different locations simultaneously, and can move rapidly. Edge-computing and real-time data are fast evolving, whereas a portion of data can be distributed within a device itself. Any policies that speak to data storage must thus be 'future proof' to accommodate such developments.[59]

The objectives of data localisation are largely worthy of pursuit: South Africa is indeed set to be further left behind in the development process if the current concentration of power in a few giant digital platforms is simply consolidated. African nations and other countries in the Global South are also rightly concerned that the political struggles that inhered in the trade liberalisation movement, as well as imbalances in international trade, will be repeated in a different guise in the context of the data revolution.[60] In a more equitable global distribution, South Africa would enjoy the necessary infrastructure and skillsets to store, process and transform data locally without the need to rely on foreign data centres. However, the global political economy is configured in such a way as to hamper new entrants – even well-positioned, potential innovation hubs such as South Africa. Given the concentration of power and barriers for countries such as South Africa to host all data value chains within its borders, it is necessary to move away from an exclusive focus on where data is stored.

South Africa can exert its data sovereignty through innovative mechanisms that ensure that it benefits from the socio-economic value data delivers when used, while adequately protecting human rights. This does not mean that South Africa should attempt to 'own' data, especially personal data which belongs to data subjects. Current language in the draft National Data and Cloud Policy that refers to data as the 'property' of South Africa, without distinguishing what types of data are being targeted or clarifying what is meant by 'South Africa' being the 'owner' of data, is counter-productive.[61] In fact, research has shown that state capacity can have a determinative impact on data localisation outcomes.[62] A severely constrained energy grid and negative economic outlook imply that South Africa does not presently enjoy the capacity needed to obtain positive outcomes from additional data localisation measures, or to be in a position where the country 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).[63] Instead, 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.[64] More emphasis should be placed on skills development, including data analytics, so that sovereignty can manifest as the creation and capture of value regardless of where data is stored. In so doing, the principle of LNOB should be observed by specifically empowering vulnerable and marginalised communities, such as women and rural communities.[65] Value can also be captured through taxation, as recognised in the draft National Data and Cloud Policy. South Africa should actively participate in the OECD process to ensure that similarly placed countries derive an equitable share of taxation of data and related digital products and services.

South Africa can exert its data sovereignty through innovative mechanisms that ensure that it benefits from the socio-economic value data delivers when used, while adequately protecting human rights.

South Africa's current conditional flow regime for personal data, as reflected in the POPIA, constitutes a balanced and moderate approach to data localisation. This approach is one that is in line with international law standards that guarantee the right to privacy on the one hand, and the free flow of information on the other. The United Nations High Commissioner for Human Rights has noted that cross-border data flows are necessary in today's globalised world, and that strict data localisation requirements should be avoided. Instead, the High Commissioner notes that data should only be transferred to jurisdictions that at least guarantee international law human rights standards.[66] Government should thus ensure that the POPIA's processing standards are consistently complied with by all stakeholders who deal with personal data. If the data protection regime is not

enforced, it is likely that individuals' constitutional right to privacy will be violated through the unlawful processing and use of their data, even if it is stored within South Africa's borders. The Information Regulator will play a key role in ensuring awareness and enforcement of processing standards as required by the POPIA. If personal data is genuinely safe and secure when processed in South Africa, public trust will improve, which can in turn filter down into *trusted* cross-border flows of data when this is preferable or more feasible than local storage. On the other hand, should stronger data localisation measures be introduced, as suggested by the draft National Data and Cloud Policy, it is possible that the right of access to information and property rights may be infringed through restrictions on the free flow of information. It is important to bear in mind that undue state surveillance and other protectionist agendas are not permitted to violate privacy rights in conflict with the POPIA.[67] In order to catalyse the capture of the socio-economic value of data through evidence-based policy making, government should invest in skills development such as data analytics, in order to empower various public bodies and organs of state to exploit the value of data for the benefit of citizens through targeted service delivery. South Africa should thus focus on developing its data protection and data policies at a national level, before moving on to contribute to regional and international efforts aimed at interoperability (rather than harmonisation).[68]

7. POLICY RECOMMENDATIONS

Before introducing further data localisation requirements that will entail trade-offs that are not necessarily in the interests of South Africa's project of sustainable development, there are several lacunae that policy makers should focus on addressing in the first instance. This includes both national, regional and international policy actions that can interact to ensure South Africa is not left behind in the data revolution.

First, government should ensure that processing standards and the conditional flow of data as set out in the POPIA, are complied with and enforced domestically. This will ensure that the right to privacy of South Africans is respected and protected. It will fall to the Information Regulator to ensure that both state and non-state actors do not overstep the bounds of personal data protection as set out in this crucial piece of legislation.

Second, government should carefully revise the draft National Data and Cloud Policy in consultation with state and non-state stakeholders, and based on public input on the draft policy. The language used in the context of data localisation is obfuscating and confusing. It does not clearly distinguish between different types and uses of data. It will also be necessary to revise the policy in a manner that demonstrates that adequate data protection and cyber security frameworks are in place, in order to attract FDI. At the same time, government should be sensitive to the fact that 'hard' data localisation requirements may lead to retaliation and avoidance in terms of FDI as well as trade. It will be necessary to actively engage in international efforts to develop an equitable global tax regime for purposes of the digital economy. South Africa must thus represent the interests of developing countries in Africa in actively engaging with the OECD's work and its two pillars, namely Pillar One – the re-allocation of taxing rights and Pillar Two – the global anti-base erosion mechanism. Domestic policy should thus not hamper efforts to develop some form of consensus on a novel and equitable tax regime in this new field.

The Information Regulator will play a key role in ensuring awareness and enforcement of processing standards as required by the POPIA.

Third, South Africa should assume a leading role in advocating for interoperability and policy coherence in Africa and globally. In the first place, South Africa should ratify the Malabo Convention and use its regional status to encourage other countries to do the same. While efforts continue to achieve some semblance of international interoperability and standard-setting, South Africa should leverage its continental position to advocate for a protocol on data flows under the AfCFTA. In addition, South Africa should consider the pursuit of equitable multilateral free trade agreements to ensure the trusted and secure flow of data, while positioning itself as a trusted processing hub. South Africa should simultaneously invest in skills beyond infrastructure, such as data analytics, to truly benefit from the 4IR and Africa's digital economy.

Finally, all relevant stakeholders should participate and cooperate in striking a balance between data protection and economic development through the adoption of a 'whole society approach' to the regulation of the data ecosystem. Thus, for example, where there is interoperability and coherence between standards contained in instruments such as the POPIA and the GDPR, MNEs should welcome such consistency for ease of compliance and doing business. Moreover, any regulation should be flexible in order to keep up with rapid developments in the field, and policy makers

should concomitantly be open to revisions and amendments in order to guarantee 'future proof' policies. Regulatory sandbox approaches, and experimentation with data stewardship models, should be actively pursued in this cutting-edge space.

8. CONCLUSION

South Africa is poised to capitalise from its regional position and boost its sustainable development agenda through benefiting from the digital economy and one of its key drivers, namely data. South Africa's current data protection framework manages to strike a sufficiently flexible policy balance between data protection and economic development with respect to personal data. However, recent policy developments appear to jeopardise South Africa's progress as a regional leader in the data ecosystem and digital economy, and may lead to perverse and anti-development outcomes. Government should accordingly focus on enforcing current data protection laws while actively seeking to develop interoperable data protection standards at the regional and international levels. Moreover, government should build its data capacities and empower vulnerable groups through investing in critical skills such as data analytics. An inordinate focus on data localisation – at the expense of equally relevant considerations – risks leaving South Africa behind in the data revolution, to the detriment of its people. At the same time, foreign jurisdictions and large digital firms should act on the duties of cooperation set out in the Sustainable Development Goals, since a global digital economy requires global solutions. A holistic and collaborative approach to data protection and inclusive economic growth is capable of spurring sustainable development, and reducing new patterns of inequalities occurring within South Africa and between South Africa and other nations in the context of the digital economy.

ABBREVIATIONS AND ACRONYMS

4IR	Fourth Industrial Revolution
ACHPR	African Commission on Human and Peoples' Rights
AfCFTA	African Continental Free Trade Agreement
CIPC	Companies and Intellectual Property Commission
DSI	Department of Science and Innovation
ECIPE	European Centre for International Political Economy
EU	European Union
FDI	Foreign Direct Investment
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
HIPSSA	Harmonisation of the ICT Policies in Sub-Saharan Africa
HPCDPC	High Performance Computing and Data Processing Centre
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communications Technology
IIF	Institute of International Finance
LNOB	Leave No One Behind
MNEs	Multi-National Enterprises
NDP	National Development Plan
NIPMO	National Intellectual Property Management Office
OECD	Organisation for Economic Co-operation and Development
POPIA	Protection of Personal Information Act
SDG	Sustainable Development Goal
SMEs	Small and Medium Enterprises
UNCTAD	United Nations Conference on Trade and Development
US	United States

ENDNOTES

1 UNCTAD, *Digital Economy Report* 2019 (Geneva: United Nations, 2019), xv.
2 Institute of International Finance, *Data Localization: Costs, Tradeoffs, and Impacts Across the Economy* (Washington DC: IIF, 2020), 1.
3 S 2 of the Constitution.
4 Ss 14; 16; and 32 of the Constitution, respectively. a
5 S 36 of the Constitution.
6 S 39(1)(b) of the Constitution.
7 UN General Assembly, *Transforming our* World*: the 2030 Agenda for Sustainable Development*, A/RES/70/1 (2015).
8 See generally The World Bank, *Overcoming Poverty and Inequality in South Africa: An Assessment of Drivers, Constraints and Opportunities* (Washington DC: World Bank Group, 2018).
9 African Union Commission, *Agenda 2063: The Africa We Want* (2015).
10 Article 15 (c) (ii) of the Protocol on Trade in Services of the AfCFTA. See further 'The Africa continental Free Trade Agreement and cross-border data transfer: maximising the trade deal in the age of Digital Economy', *Lexology*, March 17, 2019, https://www.lexology.com/library/detail.aspx?g=b257542e-7ff8-4ce9-ae70-f1508172c925.
11 S 1 of the POPIA defines 'personal information' as:
'information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to –
(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
(b) information relating to the education or the medical, financial, criminal or employment history of the person;
(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
(d) the biometric information of the person;
(e) the personal opinions, views or preferences of the person;
(f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
(g) the views or opinions of another individual about the person; and
(h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person…'
S 1 of the Electronic Communications and Transactions Act, 25 of 2002 defines 'data' as 'electronic representations of information in any form'.
12 See Sizwe Snail ka Mtuze, 'Protection of Personal Information Act (POPIA)', *Law Society of South Africa* (March 2021), 12-17.
13 See Sizwe Snail ka Mtuze, 'Protection of Personal Information Act (POPIA)', *Law Society of South Africa* (March 2021), 11. The GDPR has gained prominence and constitutes a *de facto* benchmark and gold standard for other regional and national data protection standards.
14 S 3(1)(b)(ii) of the POPIA.
15 See Sizwe Snail ka Mtuze, 'Protection of Personal Information Act (POPIA)', *Law Society of South Africa* (March 2021), 26.
16 Tim Cohen, 'Critics of SA government's proposed digital grab idea express deep concerns', *Daily Maverick*, May 3 2021, https://www.dailymaverick.co.za/article/2021-05-03-critics-of-sa-governments-proposed-digital-grab-idea-express-deep-concerns/.
17 Tim Cohen, 'Critics of SA government's proposed digital grab idea express deep concerns', *Daily Maverick*, May 3 2021 https://www.dailymaverick.co.za/article/2021-05-03-critics-of-sa-governments-proposed-digital-grab-idea-express-deep-concerns/.
18 Bertrand de la Chapelle and Lorrayne Porciuncula, *We Need to Talk About Data: Framing the Debate Around Free Flow of Data and Data Sovereignty*, Internet and Jurisdiction Policy Network (2021), 53.
19 African Union, List of Countries which have Signed, Ratified/Acceded to the Convention on Cyber Security and Personal Data Protection, https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf.
20 Graham Greenleaf and Bertil Cottier, Comparing African data privacy laws: International, African and regional commitments, Pre-print version 22 April 2020; Submitted to *International Data Privacy Law* (OUP), p. 33.

21 Bertrand de la Chapelle and Lorrayne Porciuncula, *We Need to Talk About Data: Framing the Debate Around Free Flow of Data and Data Sovereignty*, Internet and Jurisdiction Policy Network (2021). For an exposition of early initiatives to develop standards for closed networks in the 1970s and 1980s, see Christopher Kuner, 'Data Nationalism and Its Discontents', *Emory L. J. Online*, no. 64 (2015) 2089 2091. For the evolution of regional data protection standards in the European Union following the OECD Privacy Guidelines of 1980 (revised 2013), including an overview of Africa's involvement with the previous Convention 108, see generally Graham Greenleaf and Bertil Cottier, 'Comparing African data privacy laws: International, African and regional commitments', pre-print version April 22, 2020; submitted to *International Data Privacy Law* (OUP).

22 OECD, Action 1 Tax Challenges Arising from Digitalisation, https://www.oecd.org/tax/beps/beps-actions/action1/.

23 Compare, for example, Michael Kwet, 'Digital colonialism is threatening the Global South', *Al Jazeera*, March 13, 2019, https://www.aljazeera.com/opinions/2019/3/13/digital-colonialism-is-threatening-the-global-south; Rashmi Banga and Richard Kozul-Wright, 'Feeding data to digital giants is anti development', *The Hindu Business Line*, September 26, 2018, https://www.thehindubusinessline.com/opinion/feeding-data-to-digital-giants-is-anti-development/article25050293.ece; Jacqueline Hicks, "Digital colonialism': why some countries want to take contro lof their people's data from Big Tech', *The Conversation*, September 26, 2019, https://theconversation.com/digital-colonialism-why-some-countries-want-to-take-control-of-their-peoples-data-from-big-tech-123048 with Matthias Bauer et al, *The costs of data localisation: Friendly fire on economic recovery*, ECIPE Occasional Paper, No. 3/2014, European Centre for International Political Economy (ECIPE), (Brussels: ECIPE, 2014); Anupam Chander and Uyên P. Lê, 'Data Nationalism', *Emory L. J.*, no. 64 (2015): 677 read with Christopher Kuner, 'Data Nationalism and Its Discontents', *Emory L. J. Online*, no. 64 (2015).

24 Bertrand de la Chapelle and Lorrayne Porciuncula, *We Need to Talk About Data: Framing the Debate Around Free Flow of Data and Data Sovereignty*, Internet and Jurisdiction Policy Network (2021).

25 Dan Ciuriak and Maria Ptashkina, *Leveraging the Digital Transformation for Development: A Global South Strategy for the Data-driven Economy*, Policy Brief No. 148, Centre for International Governance Innovation (Canada: Ontario, 2019).

26 Jacqueline Hicks, "Digital colonialism': why some countries want to take contro lof their people's data from Big Tech', *The Conversation*, September 26, 2019, https://theconversation.com/digital-colonialism-why-some-countries-want-to-take-control-of-their-peoples-data-from-big-tech-123048.

27 Jacqueline Hicks, "Digital colonialism': why some countries want to take contro lof their people's data from Big Tech', *The Conversation*, September 26, 2019, https://theconversation.com/digital-colonialism-why-some-countries-want-to-take-control-of-their-peoples-data-from-big-tech-123048.

28 Anupam Chander and Uyên P. Lê, 'Data Nationalism', *Emory L. J.*, no. 64 (2015): 714.

29 Anupam Chander and Uyên P. Lê, 'Data Nationalism', *Emory L. J.*, no. 64 (2015): 720.

30 Karen Allen, 'Critical infrastructure attacks: why South Africa should worry', *Institute for Security Studies*, March 9, 2021, https://issafrica.org/iss-today/critical-infrastructure-attacks-why-south-africa-should-worry.

31 Michael Kwet, 'Digital colonialism is threatening the Global South', *Al Jazeera*, March 13, 2019, https://www.aljazeera.com/opinions/2019/3/13/digital-colonialism-is-threatening-the-global-south.

32 Jacqueline Hicks, "Digital colonialism': why some countries want to take contro lof their people's data from Big Tech', *The Conversation*, September 26, 2019, https://theconversation.com/digital-colonialism-why-some-countries-want-to-take-control-of-their-peoples-data-from-big-tech-123048.

33 Rashmi Banga and Richard Kozul-Wright, 'Feeding data to digital giants is anti development', *The Hindu Business Line*, September 26, 2018, https://www.thehindubusinessline.com/opinion/feeding-data-to-digital-giants-is-anti-development/article25050293.ece.

34 Rashmi Banga and Richard Kozul-Wright, 'Feeding data to digital giants is anti development', *The Hindu Business Line*, September 26, 2018, https://www.thehindubusinessline.com/opinion/feeding-data-to-digital-giants-is-anti-development/article25050293.ece.

35 Christopher Kuner, 'Data Nationalism and Its Discontents', *Emory L. J. Online*, no. 64 (2015): 2092-2097.

36 Bertrand de la Chapelle. and Lorrayne Porciuncula, *We Need to Talk About Data: Framing the Debate Around Free Flow of Data and Data Sovereignty*, Internet and Jurisdiction Policy Network (2021),11-12.

37 Anupam Chander and Uyên P. Lê, 'Data Nationalism', *Emory L. J.*, no. 64 (2015): 719.

38 Anupam Chander and Uyên P. Lê, 'Data Nationalism', *Emory L. J.*, no. 64 (2015): 717.

39 Anupam Chander and Uyên P. Lê, 'Data Nationalism', *Emory L. J.*, no. 64 (2015): 718.

40 Jacqueline Hicks, "Digital colonialism': why some countries want to take contro lof their people's data from Big Tech', *The Conversation*, September 26, 2019, https://theconversation.com/digital-colonialism-why-some-countries-want-to-take-control-of-their-peoples-data-from-big-tech-123048; Dieter Plehwe, Moritz Neujeffski and Werner Krämer, 'Saving the dangerous idea: austerity think tank networks in the European Union', *Policy and Society 37*, no. 2 (2018): 188-205.

41 China, Indonesia, Vietnam, Korea, Brazil, the EU, and India.

42 Matthias Bauer et al, *The costs of data localisation: Friendly fire on economic recovery*, ECIPE Occasional Paper, No. 3/2014, European Centre for International Political Economy (ECIPE) (Brussels: ECIPE, 2014), 2.

43 Institute of International Finance, *Data Localization: Costs, Tradeoffs, and Impacts Across the Economy* (Washington DC: IIF, 2020), 4.

44 Martina F Ferracane, *South Africa and Data Flows: How to Fully Exploit the Potential of the Digital Economy*, Discussion Paper, GEGAFRICA (April 2018), 23.

45 Institute of International Finance, *Data Localization: Costs, Tradeoffs, and Impacts Across the Economy* (Washington DC: IIF, 2020), 7.

46 Institute of International Finance, *Data Localization: Costs, Tradeoffs, and Impacts Across the Economy* (Washington DC: IIF, 2020), 2.

47 Art 20 of the Banjul Charter.

48 Arjun Sengupta, *Conceptualizing the Right to Development for the Twenty-First Century, in Realizing the Right to Development* (Geneva: United Nations, 2013), 79.

49 UNCTAD, *Digital Economy Report* 2019 (Geneva: United Nations, 2019), xvi.

50 UNCTAD, *Digital Economy Report* 2019 (Geneva: United Nations, 2019), xvi.

51 UNCTAD, *Digital Economy Report* 2019 (Geneva: United Nations, 2019), xvii.

52 UNCTAD, *Digital Economy Report* 2019 (Geneva: United Nations, 2019), xvi.

53 UNCTAD, *Digital Economy Report* 2019 (Geneva: United Nations, 2019), xvii. A distinction should be made between value creation, value addition and value capture. The latter refers to the ability of organisations or governments to keep surplus value within their borders. See further UNCTAD, *Digital Economy Report* 2019 (Geneva: United Nations, 2019), 38.

54 UNCTAD, *Digital Economy Report* 2019 (Geneva: United Nations, 2019), xviii.

55 UNCTAD, *Digital Economy Report* 2019 (Geneva: United Nations, 2019), xvii.

56 Bertrand de la Chapelle and Lorrayne Porciuncula, *We Need to Talk About Data: Framing the Debate Around Free Flow of Data and Data Sovereignty*, Internet and Jurisdiction Policy Network (2021), 15.

57 Bertrand de la Chapelle and Lorrayne Porciuncula, *We Need to Talk About Data: Framing the Debate Around Free Flow of Data and Data Sovereignty*, Internet and Jurisdiction Policy Network (2021), 12.

58 Sibhale Maling, Several Flaws in SA's draft data and cloud policy, say experts, *IT web*, June 11, 2021, https://www-itweb-co-za.cdn.ampproject.org/c/s/www.itweb.co.za/amp/content/xA9PO7NZ46Z7o4J8.

59 Bertrand de la Chapelle and Lorrayne Porciuncula, *We Need to Talk About Data: Framing the Debate Around Free Flow of Data and Data Sovereignty*, Internet and Jurisdiction Policy Network (2021), 17.

60 Bertrand de la Chapelle and Lorrayne Porciuncula, *We Need to Talk About Data: Framing the Debate Around Free Flow of Data and Data Sovereignty*, Internet and Jurisdiction Policy Network (2021), 22.

61 According to some commentaries on the draft National Data and Cloud Policy, this amounts to an attempt by government to expropriate property rights in data. See Innovus, Technology Transfer Office of Stellenbosch University, *Written Submission to the Proposed National Data and Cloud Policy in terms of the Electronic Communications Act, 2005 (Act 36 of 2005) Published for Comment 1 April 2021*, May 14, 2021.

62 Kaushambi Bagchi and Sashank Kapilavai, 'Political Economy of Data Nationalism', (paper, 22nd Biennial Conference of the International Telecommunications Society (ITS): "Beyond the Boundaries: Challenges for Business, Policy and Society", Seoul, Korea, 24-27 June, 2018, International Telecommunications Society (ITS), Calgary).

63 Compare the positive findings in respect of Facebook's data centre fleet, which demonstrates that socio-economic outcomes will vary greatly according to different country contexts: Zachary Oliver et al, *The Impact of Facebook's U.S. Data Center Fleet* (Menlo Park: Facebook, 2018).

64 Bertrand de la Chapelle and Lorrayne Porciuncula, *We Need to Talk About Data: Framing the Debate Around Free Flow of ata and Data Sovereignty*, Internet and Jurisdiction Policy Network (2021), 18.

65 UNCTAD, *Digital Economy Report* 2019 (Geneva: United Nations, 2019), xix.

66 United Nations High Commissioner for Human Rights, *The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights*, Human Rights Council Thirty-ninth session, A/HRC/39/29, para 32.

67 The use of data for law enforcement and surveillance purposes is regulated in other statutes such as the Regulation of Interception of Communications and Provision of Communication-related Information Act No. 70 of 2002 and the Electronic Communications and Transactions Act No. 25 of 2002.

68 Susan Ariel Aaronson, *Data Is Different: Why the World Needs a New Approach to Governing Cross-border Data Flows*, CIGI Papers No. 197, (Ontario: Centre for International Governance Innovation, 2018), 13.

POLICY BRIEF 02

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

Shanelle van der Berg holds a PhD from Stellenbosch University and is also a Research Fellow 2021 -2024, at Stellenbosch University, Faculty of Law, Department of Public Law

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 | 400429 | www.compressdsl.com