UNIVERSITY OF JOHANNESBURG
CCRED
CENTRE FOR COMPETITION, REGULATION AND ECONOMIC DEVELOPMENT

the dtic
Department:
Trade, Industry and Competition
REPUBLIC OF SOUTH AFRICA

SARChI
SARChI Chair:
Industrial Development

POLICY BRIEF 3: DATA GOVERNANCE MATTERS: LESSONS FOR SOUTH AFRICA

July 2020

Julius Nyamwena and Pamela Mondliwa [1]

Industrial Development Think Tank[2]

On 1st July 2020, the Protection of Personal Information Act ("POPIA") came into effect after being introduced in 2014. POPIA positions South Africa in the mainstream of relatively well-developed data protection laws, regulating the collection, processing, and sharing of personal information. These controls over the use of personal data are but one aspect of data governance that countries around the world are implementing.

In addition to POPIA, South Africa needs an overarching data governance policy framework. A comprehensive data governance policy includes guidelines and laws to address data security, cybersecurity and cybercrime; the cross-border flow of personal and non-personal data; ownership of data; access to data, markets and platforms; and algorithm accountability.

Data governance matters because of the central role played by data in value creation in the information age as well as the increased data collection that is arising from digitalisation. While in previous industrial revolutions it was control of physical resources that was the most obvious determinant of value creation and capture, in the information age, this has become data. As a result, countries around the world are grappling with developing data protection laws and governance frameworks that are best suited for their particular contexts.

This brief focuses on the regulation of the flow of data across borders. It considers the options that are available to South Africa and makes recommendations based on local context and international trends. The brief draws on discussion papers and notes presented at the Expert Panel on Regulation of Digital Platforms for Economic Development, hosted in March 2020 by the Industrial Development Think Tank at CCRED.[3]

[1] Researchers at Centre for Competition, Regulation and Economic Development (CCRED), University of Johannesburg. All errors are the authors' own.

[2] The Industrial Development Think Tank (IDTT) is supported by the Department of Trade, Industry and Competition (the dtic) and is housed at CCRED in partnership with the SARChI Chair in Industrial Development at the University of Johannesburg.

[3] See Macmillan, R. (2020). Data governance: Towards a policy framework. Discussion paper prepared for Expert Panel on Regulating Digital Platforms for Economic Development, CCRED.

To localise or allow free flow of data?

Arguments for the free flow of data are part of a package of digital obligations, commonly referred to as the Digital Two Dozen, being promoted by signatories of the Trans-Pacific Partnership with the aim of creating a free flow of goods, services, and data across a free and open internet.[4] These obligations include prohibiting digital customs duties, enabling the free flow of data, preventing localisation requirements, eliminating tariffs on all manufactured goods, barring requirements for technology transfer and refraining from demanding access to source codes.[5]

There are advantages to cross-border flows of data and countries adept at fostering digital activity have witnessed increased investments through the emergence of new industries as well as the accelerated development of traditional sectors.[6] For instance, South Africa can benefit from investments in data centres which have positive economic impacts in terms of productivity, employment creation, innovation and improved competitiveness.[7]

On the other hand, some developed and developing countries are concerned that the free and open digital commerce that the Digital Two Dozen seeks to create will entrench early mover advantages of platforms and businesses from developed economies, undermining the development of developing country competitors. This can also have the effect of reducing the bargaining power of those producing the input (data), particularly in developing countries where the laws and regulations over the ownership of data and the capacities to use it profitably are weak or missing altogether.[8]

The response from both developing and developed economies has been to put in place a range of policies to govern data generated within a country, including its geographic storage. Two broad approaches have been followed. First, **data sovereignty** ensures that the laws and governance structures of a country apply to all data generated in a country, regardless of its location. Second, **data localisation**, which goes a step further by requiring that collection, processing, and storage occurs in the national boundaries.

The data localisation policies can take a variety of forms. Stringent data localisation requires that all data generated in a jurisdiction is stored and processed within the national boundaries. The 'negative list approach' to localisation requires that data should be stored and processed within the national boundaries with exceptions in some sectors or countries where data can be stored and processed outside with a copy stored within the national boundary. The 'positive list approach'

[4] The signatories are Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, Vietnam, and the United States.

[5] The Office of the United States of America Trade Representative. (2016). The Digital 2 Dozen. https://ustr.gov/sites/default/files/Digital-2-Dozen-Final.pdf

[6] Sampath, P. G. (2019). Regulating the digital economy: Dilemmas, tradeoffs and potential options, Geneva: South Centre.

[7] Bell, J. and Mondliwa, P. (2020). Data centres: How digitalisation and green investments come together. CCRED, IDTT Policy brief 2.

[8] Banga, R. and Wright, R. K. (2018). Feeding data to digital giants is anti-development. https://www.thehindubusinessline.com/opinion/feeding-data-to-digital-giants-is-anti-development/article25050293.ece

allows for the free flow of data with the exception of selected sectors where data must be localised and cannot leave the country’s borders.

Various countries have adopted different strategies with the bulk of data policies assessed allowing the free flow of data with a positive list of sectors to be localised – commonly health, banking and to a lesser extent personal data (Table 1). There is also a growing number of countries that are adopting data sovereignty often in addition to a partial localisation policy.

Table 1: Data localisation and sovereignty policies in selected countries

Data policy	Primary risks addressed by policy	Countries adopting the policy
Stringent localisation	Network security and personal data	Russia, Vietnam, Colombia, Greece
Partial localisation approaches (strategic sectors included in positive list)		
• Health: requires personal health records to be stored locally	Privacy	Australia, China, Denmark, Japan, South Korea, Canada, India
• Banking and business records: requires all banking and transactions information to be processed locally	Spam, malware and cyber-attacks	Belgium, China, Brazil, Nigeria, Philippines, Denmark, Sweden, United Kingdom, New Zealand
• Personal: requires all personal information to be stored and processed locally	Risk to individual data and cyber-attacks	Turkey, Malaysia, Russia, South Korea
Sovereignty	Cybersecurity and national security	Argentina, Denmark, Japan, South Korea, Malaysia, Taiwan, Turkey, France, Rwanda

Source: Adapted from Banga, R. (forthcoming 2020). South-South Cooperation for Building Data Infrastructure. UNCTAD Research Paper Series.

What is common across health, banking and personal data are that it is considered as sensitive given that it allows insights into an extremely intimate aspect of individuals. The rationale for local hosting of this data is that it enhances its privacy and security by ensuring that an adequate level of protection is provided and reduces the need to rely on mutual legal assistance treaties to obtain access which can delay interventions towards solving various challenges and conducting investigations. When it comes to health data there are also benefits from big data analysis of anonymised data for purposes of medical research and this is acknowledged by some of these countries with specific guidance on how data could be shared and protected for international research programmes, with requirements on keeping local copies.

Data sovereignty ensures that all data generated in a country enjoy these protections and South Africa should consider its adoption. Given the general concerns about privacy, cybersecurity and even national security taken together with the mounting evidence on the ineffectiveness of individual consent, it is imperative that countries protect their data through an appropriate legal framework. This is equally important for data that is located in foreign servers.

On data localisation, there are a number of factors to be considered including the benefits of maintaining openness for trade, innovation, and value creation; the efficiency benefits from real-time processing, which requires data centres to be located closer to users; the costs of data infrastructure investments in every country; the benefits of regional data hubs; and the sensitivity of different types of data. The balancing of these and other relevant factors may not necessarily lead to a uniform answer across different types of data and as such identifying strategic sectors and/or categories of data that require localisation is the pragmatic approach.

Does POPIA regulate cross-border flows of data?[9]

POPIA already has provisions relating to the cross-border flow of data in Chapter 9 of the Act. In terms of POPIA, a responsible party may not transfer personal information about a data subject to a third party in a foreign country unless a number of conditions are met. These conditions include that consent must be provided by the data subject; that the third party is subject to regulations or corporate rules that provide similar protection to POPIA; the transfer is necessary for the performance of a contract; or, the transfer is in the benefit of the data subject who normally is not in a position to provide consent but would grant it, where practical to do so.

There are a few limitations to this approach. First, there is increasing recognition that the consent (notice and control) solution to empower individuals is generally inadequate. Consumers simply cannot keep up with the volume, complexity and uncertainty of information about how data about them is used, what the risks are, and what trade-offs they should consider when invited to click a consent button. The all or nothing framing of users' consent, also leaves them with little choice but to click "I agree" when signing up for digital services. It is not clear that the broken model of 'notice and control' can be solved by attempting to improve notices and ensure even more explicit consent. In this regard, POPIA could be enhanced by adopting ways of shifting the burden from the individual to service providers.

Second, POPIA has not imposed a requirement, that is in place in many other countries, which requires the information regulator to confirm in advance which countries have laws providing data protection adequate to qualify for data transfers. The implication may be that the 'responsible party' has the discretion to decide which regulations and corporate policies are adequate. This could be addressed by developing standard binding corporate rules and standard contractual clauses for use by organisations seeking to transfer data in and out of South Africa. Better yet, data sovereignty addresses this challenge without the complexities of comparing data governance regulations and corporate rules. It also creates certainty, thereby reducing compliance costs.

Third, while POPIA addresses some of the concerns that data localisation and sovereignty correct for, this is only done for personal data. The implication is that the regulation of non-personal data is subject to private contracts, which can be skewed by differences in bargaining power. For example, does the data collected from sensors on leased machines belong to the user of the machine or the owner of the machine? Are platforms required to share data collected on sales and consumer behaviour to particular suppliers? Taking it a step further, do the suppliers have recourse if the platform uses the data to create own brands that can then replace the supplier? in

[9] See Macmillan (2020) for a more detailed assessment.

this regard, non-personal data can also enable entrepreneurs to develop new and innovative services and products from which citizens may benefit.[10]

The discussion above shows that South Africa needs to develop a broader data governance framework that cuts across technical governance of the collection, processing and flow of data; privacy cybersecurity; data ownership and access. Other issues not discussed in the brief include interoperability and portability (to support competition and collaboration).

[10] Indian Ministry of Electronics & Information Technology (2019). Report by the committee of experts on non-personal data governance framework.