UNIVERSITY OF JOHANNESBURG

CENTRE FOR AFRICA-CHINA STUDIES

Policy Brief

South Africa's Data Sovereignty Regulations: Merits and Possible Limitations

2

Emmanuel Matambo and
Edmund Terem Ugar

September 2022

POLICY BRIEF 2

Centre for Africa-China Studies
University of Johannesburg

Policy Brief No 2

South Africa's Data Sovereignty Regulations: Merits and Possible Limitations

Emmanuel Matambo and Edmund Terem Ugar

Published in September 2022 by:
The Centre for Africa-China Studies (CACS)
at the University of Johannesburg
9 Molesey Avenue
Auckland Park
Johannesburg
South Africa
www.cacs.org.za

For enquiries, contact:
Dr. Emmanuel Matambo
– Research Director, CACS
Tel: +27 11 559 7675
Email: ematambo@uj.ac.za

POLICY BRIEF 2

South Africa's Data Sovereignty Regulations: Merits and Possible Limitations

Emmanuel Matambo and Edmund Terem Ugar

1. Introduction and Background

Many ethical guidelines, values and principles have been published by the United Nations to govern data extraction and mining for technological research and development. These principles are: privacy, autonomy, human rights, accountability, diversity, trust, fairness, and others. These guidelines protect the data extracted from individuals for technological research and development. However, while these principles and guidelines are necessary for the protection of individuals against unlawful data extraction and mining, there is a contention that, firstly, they do not, in practice, apply to all contexts, given the socio-political and economic differences between developed countries in the global North and developing countries in the global South, especially in sub-Saharan countries like South Africa. As a result, issues such as "surveillance capitalism" – the extraction of human source data for profit creation (Zuboff, 2015:75) – and "data colonialism" – a process of combining the "predatory extractive practice of historical colonialism with the abstract quantification methods of computing" (Couldry and Mejias, 2018:2) – both flourish in sub-Saharan Africa with actors such as Silicon Valley, despite the aforementioned ethical guidelines.

Given the issues of surveillance capitalism and data colonialism, in July 2021 South Africa took proactive measures to ensure data sovereignty by enforcing the 2013 Protection of Personal Information Act (POPIA). In line with the measures for personal data protection, the South African government published the National Cloud and Data Policy in April 2021 as a further step toward achieving data sovereignty. However, there are still lacunas identified in this paper that need to be rectified in policies such as the POPIA to ensure maximum protection of private data, as well as achieve robust data sovereignty in the country.

The first section discusses the importance of data in the current social milieu. The paper begins by explaining what big data means. Afterwards the paper shows why there is a need for data sovereignty in South Africa. The second section engages with South Africa's measures to enforce data laws, such as the POPIA. The third section discusses the limitations of the POPIA document. The final section makes recommendations based on the identified limitations. The Final section concludes the paper.

2. Data Sovereignty

Big data has become an important aspect of our societies in our current social milieu due to its vital role in technological structures and the production of the technologies of our current industrial age, like artificial intelligence and robotics. The enormous generation and flow of data due to the ubiquity and proliferation of our electronic devices such as our cell phones, iPad, laptops, and smartwatches can be tied to the Internet of Things (IoT) – that is, the interconnectedness of devices. This data flow has resulted in datafication – the processing of information of whatever kind into quantifiable data for different purposes (Mayer-Schonberger and Cukier, 2013). Data is generated from different sources: paper surveys, the information we share verbally, and information from our devices such as smartphones, text messages, video recorders, and personal computers (Aaronson, 2021).

The United Nations Conference on Trade and Development (UNCTAD, 2021) reports that big digital companies extract data worth 230 exabytes, an equivalent of 230 billion gigabytes, monthly in 2020. This implies that 30 gigabytes of data are generated monthly by one of the 7.9 billion people that currently exist in the world. The extraction of personal data for research and development purposes by the big players in technological infrastructures such as Silicon Valley has resulted in what has been theorised as surveillance capitalism and data colonialism. Due to this new form of colonialism there has been a call by different nation-states to put stringent measures and policies in place to advance the protection of personal data within their territory and even beyond. This measure has been termed data sovereignty.

Data sovereignty is the authority, governance, and management of data by nation-states through the formulation of policies, laws, and regulations to guide the generation and flow of personal and non-personal data within the jurisdiction of the states for economic, strategic interests and national security purposes (Polatin-Reuben and Wright, 2014; Couture and Toupin, 2019; Floridi, 2020; Hummels et al., 2021). Data sovereignty has become crucial as many nation-states actively engage in reclaiming the governance of their cyberspace from private sectors due to the economic and political benefits of data. Further steps by the state to take ownership of their cyberspace involve the inclusion of cyberspace as the fifth domain of warfare "after land, sea, air, and space" (Broeders and Van De Bergh, 2020: 1). Besides the importance of data to the security sphere, there is the economic importance of data such as the prospect of increased productivities, developments, and accountability in governance (McKinsey Global, 2013; World Bank, 2021; World Economic Forum, 2021). In what follows, this paper now engages with the measures the government of South Africa has put in place to ensure its data sovereignty.

3. Data Sovereignty and the POPI Act in South Africa

The South African POPIA was promulgated in 2013 and the Act took effect in 2021. The POPIA sets out the regulations and laws relating to third parties involved in data processing, such as the collection, use, transfer, matching and storage of data. Besides the POPIA, other regulatory bodies such as the Electronic Communication Act of 2002 and the Promotion of Access to Information Act of 2000 have been put in place to regulate the generation and flow of data within the South African context. In the POPI Act, the phrase "processing of information" appears frequently, so it is pertinent to dissect what the phrase means in data ethics and laws.

The POPI Act outlines eight conditions for the lawful processing of data which are:

1. Accountability: those responsible for lawful processing of personal data must comply with the conditions stated in the POPIA for determining the purpose of processing and during processing (Section 8).
2. Process Limitation: parties involved in processing personal information must ensure that they provide a clear definition of their purpose of collecting personal data, and after the said purpose has been achieved they must ensure to destroy the collected data. Furthermore, consent must be given by the data subject before collecting and processing their personal information (Section 9-12).
3. Purpose Specification: If there is a need for collected data to be used outside the initial defined purpose, parties involved in the data collection must specify and also state what purpose the data will be used for and the duration (Section 13-14).
4. Further Processing Limitation: collected personal data can be used for research only if the aforementioned condition has been met (Section 15).
5. Information Quality: parties must ensure that the collected data must not misleading. As a result, the collected data must be accurate and up to date (Section 16).
6. Openness: those responsible for data collection must maintain a record of all processing of personal information. These parties must ensure that they specify the reason for collecting the data, those involved in the collection of the data, the access rights of the data subject to delete/correct their data, and if there is an intention to transfer the data to third parties during the time of processing (Sections 17-18).
7. Security Safeguards: personal information of data subjects must be secured to maintain integrity, confidentiality, and data breaches (Section 19-22).
8. Data Subject Participation: data subjects must be informed about their rights to their data and the accessibility to alter their data however they deem fit (Section 23-25)

The principle of consent plays an important role in the POPI Act. The principle of consent goes concomitantly with the principle of explainability. Here explainability means explaining to data subjects their rights to withdraw their consent, change, or

delete their data. However, the Act states that data from social media spaces can be processed without the consent of the data subject if the data is published in public domains. However, when it comes to private information shared between two parties or more in private social media spaces such as WhatsApp messenger, the data of this sort is private and ought to be respected at all times. Furthermore, other special private information or high-risk information identified by the POPI Act, which includes religious or philosophical beliefs, political persuasion, biometric information, health or sex life, and trade union membership of data subjects, must be respected at all times.

4. POPIA Cross Border Data Transfer Regulations

The POPI Acts regulations state that the data of a subject cannot be transferred to a third party in a foreign country unless the foreign country has the following measures in place: First, the foreign country acts in accordance with the EU General Data Protection Regulation, such as human right regulations and other data protection laws which is similar to the POPI Act. Second, there has to be proof of a binding corporate rule(s) which ensures the protection of the information of the data subject. Third, there must be a clear written agreement between the sender and the receiver of the data. Fourth, data subjects must consent to allow the transfer of their information abroad.

5. Limitations of the South African Data Regulations

There are several limitations that this paper identifies in the South African data regulations policy. These limitations are: First, the policies are embedded with long terminologies and jargon that are not easy to decipher by lay people. Second, data exploitation results from language and communication barriers – if the lay people are ignorant of the terminologies, it follows that there will be an opening for exploitation. Third, at the moment one cannot in practice differentiate the state and big capital companies in processing data because a clear line has not been drawn. Fourth, the POPI Act states that data subjects must give their consent before their data is processed and used, and if the data will be reused, they must still ask for the data subject's consent. However, the Act does not clearly state when the data will be destroyed after use.

6. Recommendation

South Africa can leverage the benefits of big data in education, security, transportation, manufacturing, and policy development if the country can harness its potential with a robust data regulation law. However, the state should not lose focus in terms of protecting the private information of its citizens while trying to utilise the market benefits of big data for research and development purposes. Given the limitations spelled out above, one way to mitigate the risk of private information abuse is that the government must take a proactive step to ensure that the language of communication

in avenues that involve the collection of personal data is made most succinctly and simplistically possible. Second, there should be a clear line between the government and private big digital capital companies. The former must ensure it has adequate laws in place to protect the private information of South Africans, and the latter group must be forced to oblige to the regulations to avoid surveillance capitalism and data colonialism. Finally, there must be a specified timeframe when collected data should be destroyed, especially data that is transferred to third parties for processing.

7. Conclusion

This paper has discussed the growing interest in data sovereignty amongst nation-states with a particular focus on South Africa. The paper engages with the South African data regulations such as the POPIA to see its merit and demerit. Finally, the paper makes some recommendations to ensure a robust data protection policy and data sovereignty in South Africa.

Reference List

Aaronson, S.A. 2021. Data is disruptive: How data sovereignty is challenging data governance. *Hinrich Foundation*.

Broeders, D. and Van Den Bergh, B. 2020. Governing Cyberspace: Behaviour, Power, and Diplomacy. In Broeders, D. and Van Den Bergh, B. (Eds.), *Governing Cyberspace: Behaviour, Power, and Diplomacy.* Lanham: Rowman and Littlefield.

Couture, S. and Toupin, S. 2019. What does the notion of "sovereignty" mean when referring to the digital? *New Media and Society*, 00(0), pp. 1-18.

Couldry, N., & Mejias, U. 2018. Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. *Television and New Media*, Vol. 33, No.4, pp. 1– 14.

Floridi, L. 2020. The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philosophy & Technology*, 33, pp. 369–378.

Hummel, P., Braun, M., Tretter, M. and Dabrock, P. 2021. Data sovereignty: A review. *Big Data and Society*, pp. 1-17.

Mayer-Schonberger, V. and Cukier, K. 2013. *Big Data: A Revolution That Will Transform How We Live, Work and Think.* New York: Houghton Mifflin Harcourt Publishing Company.

McKinsey Global Institute. 2013. Open data: Unlocking innovation and performance with liquid information. Available at https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/open-data-unlocking-innovation-and-performance-with-liquid-information.

Polatin-Reuben, D. and Wright, J. 2014. *An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet*. 7 July 2014, University of Oxford.

Republic of South Africa. *Protection of Personal Information Act (POPIA) 2013*. Government Gazette, Available at https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf.

United Nations Conference on Trade and Development (UNCTAD). 2021. *Cross-border data flows and development: For whom the data flow. Digital Economy Report 2021.* United Nations, Geneva. Available at https://unctad.org/webflyer/digital-economy-report-2021.

World Bank Group. 2021. *Data for Better Lives*. World Development Report 2021. Washington: The World Bank.

World Economic Forum (WEF). 2021. Data-Driven Economies: Foundations for Our Common Future. White Paper, April 2021. Available at https://www3.weforum.org/docs/WEF_WP_DCPI_2021.pdf.

Zuboff, S. 2015 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*, Vol.30, No.1, pp. 75– 89.