POLICY BRIEF

Data Regulation in Africa: Free Flow of Data, Open Data Regimes and Cyber Security

Hanani Hlomani and
Caroline B. Ncube

February 2022 / No.DG004

The Context

The free flow of data, the adoption of open data regimes and cyber security are three major aspects of data regulation that hold the reigns to the potential development of the continent. This policy brief addresses these aspects in Africa with a focus on regulatory instruments from the different bodies at continental and sub-regional level as well as some national legislation from selected countries. The aim is to draw lessons from the European Union (EU) approach to determine an appropriate African centred approach to data regulation, particularly in the context of increased inter-African trade as envisaged by the

Agreement on the African Free Continental Trade Area (AfCFTA) and an enhanced digital economy as motivated for in the Digital Transformation Strategy for Africa (2020 – 2030).

The problem

Lighting pace technological advancements have made it difficult for legal scholars, policy drafters and legislators to stay abreast with all the considerations and important policy debates that are necessary to ensure that the law is not outpaced and eventually invalidated by technology. Data has emerged as a key resource especially following the COVID-19 pandemic. However, the true value and utility of data can only be unlocked when such data is able to move freely and can be used/interpreted by a multitude of users. This creates a legal conundrum for those tasked with legislating on data, who have the task of producing sound policies and legislative instruments that ensure that such data can move freely, that such data is legal and not impeding on any personal or commercial interests and further that such data exchanges are done in a safe digital environment and protected against cyber-attacks. Continentally, the African Union (AU) in 2014 adopted the Convention on Cyber Security and Personal Data Protection (Malabo Convention), which focused on personal data and cyber security. Some of the Regional Economic Communities (RECs) have also adopted relevant instruments. However, outside of this concerted effort, very little has been done in terms of a collective continental/regional legislative instrument on the regulation of data, which encompasses protection of personal data as well as ancillary rights and interests that do not necessarily pertain to personal data.

Background

In a broad sense, this policy brief addresses the concerns associated with data regulation on the African continent, specifically. three major aspects that hold the reigns to the potential development of the continent. These are the free flow of data, the adoption of open data regimes, and cyber security. The brief focuses on Africa, with a focus on regulatory instruments from the different bodies at continental and sub-regional level as well as some national legislation from countries that have developed any legislative instruments that address the same concerns. Emphasis will also be paid to the strides that have been taken by the EU, the first continental body that has taken a geographically concerted approach to comprehensive data regulation. The aim is to draw lessons from such efforts with the intention of determining an appropriate African centred approach to data regulation, particularly in the context of increased inter-African trade as envisaged by the Agreement on the AfCFTA and an enhanced digital economy as motivated for in the Digital Transformation Strategy for Africa (2020 – 2030).

Research results

The research paper which informs this policy brief was written by way of desktop research over a period of approximately 6 months. A total of 68 academic articles, think pieces, policy briefs and laws were analysed. A possible caveat in the research was that from an African perspective, not a lot of literature exists on the topic of data governance. It is for this reason that a comparative approach was adopted with the EU being the main point of reference owing to their advanced efforts at data governance. The research revealed that while some countries allow data to freely flow in and out of their borders, many others have enacted legislative frameworks that speak to the protection of personal data and which contain, in most instances, data localisation clauses. Data localisation laws are often necessitated by concerns relating to data security. Such laws aim to ensure, through surveillance and other supervisory methods, that where data must be exchanged, that such data is lawfully obtained (through freely given consent), that the data is being used/exchanged for a specific purpose, and that the data is not being used for unauthorised activity such as profiling or surveillance by governments or any other third parties without consent (unless otherwise required under the law). In today's digital and physical economies, the freedom to move data of both a personal and non-personal nature without restriction between countries generates positive outcomes for organisations, individuals and countries. It was also revealed that open standards/policies for data can also be particularly useful tools that make it easier for individuals and organisations to access, use, publish and share better quality data while simultaneously addressing cyber security concerns. A well-crafted data governance framework ought to include both aspects because security and privacy have become one of the crucial concerns related to data storage and usage within organisations. Furthermore, and leading up to the adoption of the Malabo Convention in 2014, several RECs adopted regulatory instruments on privacy and cybersecurity.

The research paper found that two scenarios are happening on the continent. First, On the one hand, concerted continental efforts may be unrolling sluggishly while the data revolution is unfolding at a much faster rate. Because this is the case, progressive nations, in a bid to compete within the data economy, have elected to attempt data governance on their own, thereby proffering the present situation of discordant and possibly conflicting data regulation laws. While on the other hand, what we may be witnessing is a lack of trust and confidence amongst African states in unified regulatory efforts. In some instances, because the data that is of the highest value is personal, such a lack of trust may be coupled with paranoia and suspicion. From a regulatory perspective, it makes it exceedingly difficult for state governments to implement policies and to co-operate across borders where there is no common goal or sense of camaraderie. Some scholars have even argued that the delays in the adoption of the

Malabo convention are possibly linked to a lack of trust and paranoia around giving other nations access to their data which they fear may be used against them. Where this is the case, more harm is done than good, from a public good perspective, as the potential to harness the power of data is mewed up.

Implications for policy makers

It will therefore be imperative that a trusted data environment that grounded in the rule of law; comprehensive institutional arrangements and regulations; and competent institutions responsible for overseeing the use of public and private data is established as soon as possible. Such an environment can be created through multistakeholder efforts to improve data access and use. This may mean active dialogue between governments, consultations and collaborations with the private sector, and the establishment use of Data Protection Authorities (DPAs) competent in the investigation and prosecution of cross border breaches. On top of the inter-governmental dialogue agenda should be the negotiation of mutual assistance agreements that will guarantee similar protection of data in contracting member states and pledges to investigate and prosecute cross border cybercrimes comprehensively. Capacity-building in relation to data protection, cybersecurity and institutional data governance in relevant agencies should be prioritised and realised through policy and asset allocation. In addition, where institutional arrangements and regulations come about as a result of the consultations and dialogue, these arrangements ought to be established through inclusive, consultative and transparent processes. Accountability and transparency are the answer to most of the concerns that follow the shift to data liberalisation and use. Therefore, given the potential benefits that open cross border flows would bring about, it would be prudent to start aligning policy with the promotion of open cross border data flows. There is a need to adopt a cohesive legal approach that is unambiguous and offers protection and obligations across the continent while taking cognisance of the value that the liberalisation of data has. Going forward, existing legal instruments should be revisited regularly, where necessary, to eliminate conflicts in law and to keep abreast with the latest levels of protection and obligations within member states.

Mission

To strengthen local capacity for conducting independent, rigorous inquiry into the problems facing the management of economies in sub-Saharan Africa.

The mission rests on two basic premises: that development is more likely to occur where there is sustained sound management of the economy, and that such management is more likely to happen where there is an active, well-informed group of locally based professional economists to conduct policy-relevant research.

www.aercafrica.org

Learn More

www.facebook.com/aercafrica

www.instagram.com/aercafrica_official/

twitter.com/aercafrica

www.linkedin.com/school/aercafrica/

Contact Us
African Economic Research Consortium
Consortium pour la Recherche Economique en Afrique
Middle East Bank Towers,
3rd Floor, Jakaya Kikwete Road
Nairobi 00200, Kenya
Tel: +254 (0) 20 273 4150
communications@aercafrica.org