Blog

Data Governance Echoes

Advancing Sustainable Cross-border Data Transfer Policies and Practices in Africa

NIYEL
—CHANGE CREATORS—

CIPESA

LUX | MEA | LEX
SIGILLUM UNIVERSITATIS CHEIKH ANTA DIOP DAKARENSIS

Over the years, several African governments have enacted laws and policies that limit cross-border data flows, citing the need to protect national security, promote the local digital economy, and safeguard users' privacy. The limitations range from complete bans on cross-border transfers of all data to conditional cross-border transfer of certain data, with authorization sought from relevant government bodies.

The legal provisions prohibiting cross-border data transfers are scattered in different legal frameworks in countries such as Ethiopia, Nigeria, Rwanda, and Uganda, whose limitations are contained in their financial services and cybersecurity laws. In Rwanda, for exaample, Article 3 of Regulation No. 02/2018 of 24/01/2018 on cyber security provides that any bank licensed by the Central Bank must maintain its primary data within the territory of Rwanda. In Uganda, Article 68 of Uganda's National Payment Systems Act 2020 requires all electronic money issuers to establish and maintain their primary data centre in relation to payment system services in Uganda.

For other countries such as Kenya, Nigeria, South Africa, Tunisia, and Uganda, the limitations are contained within their data protection laws. For example, sections 48 and 49 of Kenya's Data Protection Act 2019 prohibit cross-border transfer of personal data to a country lacking appropriate data security safeguards. South Africa's 2013 Protection of Personal Information Act prohibits cross-border data transfers without the data subject's consent or unless the foreign country is believed to have adequate safeguards. In Nigeria, sections 41-43 of the 2023 Data Protection Act sets conditions under which cross-border data transfers may occur such as the requirement for the destination country to have data protection safeguards and consent from the data subject, among other conditions.

Critics of these data localization provisions and practices have often argued that the current data localisation policies and practices are not pro-people as they do not mitigate any genuine cybersecurity or online targeting but instead serve to undermine personal data privacy by facilitating government agencies' unrestricted access to citizens' personal data, including for purposes of conducting state surveillance.

These practices do not also conform to the key provisions of the 2019 African Commission on Human and Peoples' Rights (ACHPR) Declaration of Principles on Freedom of Expression and Access to Information in Africa, which prohibits countries from adopting laws and other measures that criminalize and encryption practices, including backdoors, key escrows, and data localisation requirements unless such measures are justifiable and compatible with international human rights law.

The legal data localization requirements have been identified as the most restrictive and disruptive barriers to international trade, pushing foreign registered businesses to incur extra and unnecessary costs of establishing multiple infrastructures such as local data centres and in each of their countries of operation as opposed to having one center in their country of choice. In addition, the "limited policy and regulatory reforms to facilitate the interconnection of networks across borders, including national and commercial backbones, or supervisory frameworks for data protection, data storage/processing/handling" were identified as additional weaknesses in achieving Africa's economic potential.

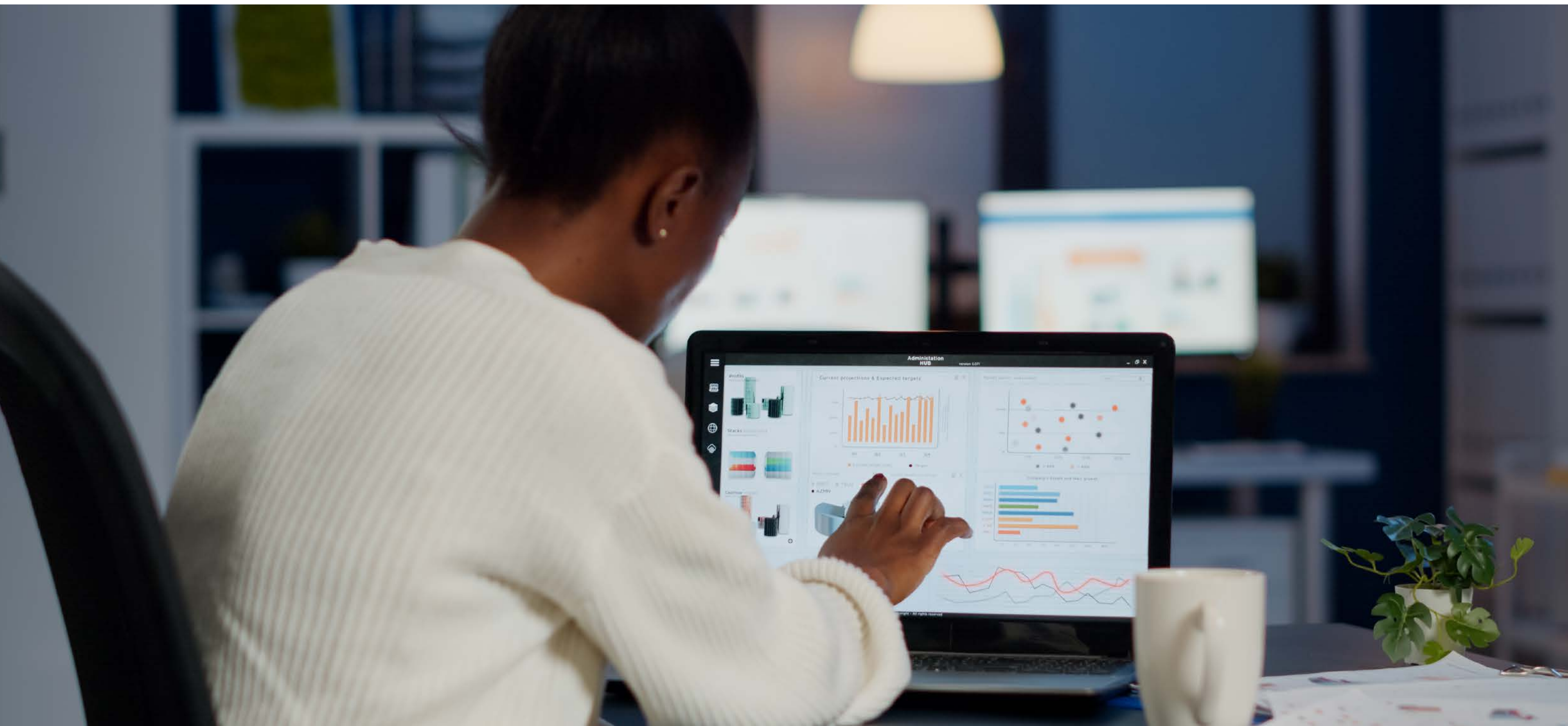
The success of several initiatives, such as the African Continental Free Trade Area (ACFTA) whose mandate is to create "a single continental market with a population of about 1.3 billion people and a combined GDP of approximately US$ 3.4 trillion," hinges on eliminating trade barriers and the harmonization of cross-border transfers through the amendment of restrictive data localisation policies and practices.

In addition, under the African Union's Digital Transformation Strategy for Africa (2020-2030), countries are called upon to "promote open data policies that can ensure the mandate and sustainability of data exchange platforms or initiatives to enable new local business models, while ensuring data protection and cyber resilience to protect citizens from misuse of data and businesses from cybercrime."

On the other hand, the AU Data Policy Framework requires countries to create an enabling legal environment that would achieve and maximize the benefits of a data-driven economy by encouraging private and public investments necessary to support data-driven value creation and innovation. The framework offers guidance on policy interventions to optimise cross-border data flows and harmonise data governance frameworks. In terms of cross-border data governance and transfers, Principle 14(6)(a) of the African Union Convention on Cyber Security and Personal Data Protection prohibits data controllers from transferring "personal data to a non-Member State of the AU unless such a State ensures an adequate level of protection of the privacy, freedoms, and fundamental rights of persons whose data are being or are likely to be processed."

A critical challenge for the continent is how to translate and localise these initiatives into workable solutions. Most autocratic governments are reluctant to amend their laws to be more open to cross-border data transfers. The reluctance is based on unfounded fears that sending their citizens' data abroad could increase citizens' vulnerability to serious security and privacy threats from foreign actors. On the other hand, civil society actors lack the requisite skills and knowledge to proactively engage in strategic advocacy both at national and regional levels. In addition, there is a paucity of evidence-based research on the key issues around data localization, particularly how various countries are implementing their data localisation policies as guided by the AU Data Policy Framework and Digital Transformation Strategy.

Lessons from previous policy advocacy engagements show that national governments are open to progressive policy reforms, as evidenced by the rapid adoption of data protection laws, particularly if they trust that such measures will not injure their national interests.



KEY INTERVENTIONS

Even with this promise and the abundance of international and regional frameworks to guide the adoption and implementation of progressive national data governance frameworks, interventions would require the adoption and implementation of multiple and mutually reinforcing strategies such as (a) building research and advocacy capacity of digital rights and data rights actors; (b) undertaking research and policy analysis; and (c) engaging in national and regional policy processes on data governance regulation, particularly that related to cross-border data flows and harmonisation of data governance frameworks.

Building on the success of her previous work on data governance and engagement with the AU Union Data Policy Framework, under the current project, the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) is continuing with regional engagements as well as working in five countries – Cameroon, Ghana, South Africa, and Uganda, to build the capacity of country-based research partners as well as generate evidence that addresses fears that informs states' restrictive regulatory stances, shows benefits of free data flows and policy harmonisation.

1. Capacity Building in Research and Advocacy

Central to CIPESA's interventions is the need to generate a critical mass of engaged actors that understand the cross-play of national and regional policy frameworks on data regulation and their implication for data policy harmonization and national policy and practice. Further, these actors will need the skills to research and produce evidence to inform engagements with actors such as policymakers and to conduct effective, collaborative advocacy to inform policy-making.

2. Research and Policy Analysis

CIPESA also supports country-based research partners to produce and communicate research-based commentaries, briefs, policy analyses, and think pieces on data localisation regulation and cross-border data policies and advocate for flexible cross-border data flows and respect for data privacy. These outputs will inform engagements with policymakers at national and regional levels and with multilateral treaty bodies that mandate data protection and monitor privacy and data rights.

3. National and Regional Advocacy and Engagement

The third strand involves strategic deployment of the published commentaries, analyses, and think pieces to attract the attention of state and non-state actors and form the basis of deliberations on how to improve the policy and practice around data governance in the region, notably on cross-border data flows, data harmonisation, and the need to embrace the AU Data Policy Framework. The advocacy will target national actors, such as data regulators, telecom regulators, and policymakers, as well as regional entities, such as the African Union, the African Commission on Human and People's Rights, and regional regulators' and telecom operators' associations such as Compassionate Rural Association for Social Action (CRASA) and East African Communication Organisations (EACO).

By building on pivotal and live continental initiatives such as the AU Data Policy Framework, the Digital Transformation Strategy for Africa, and the African Continental Free Trade Area (ACFTA), and working at regional and four-country levels through a multi-sector network of actors, CIPESA hopes to generate evidence demystifies the unfounded fears that inform states' restrictive cross-border data regulatory policies and practices while demonstrating the benefits of free data flows and proposing harmonisation measures.

Paul Kimumwe
Senior Program Officer/ CIPESA

CONTACTS:

Paul Kimumwe
E mail: paul@cipesa.org
https://cipesa.org

Niyel
E mail: info@niyel.net
www.niyel.net