Symposium on the Economic Impacts of Data Localisation in Africa: Data Localisation in Kenya: Potential Economic Impact and Effect on Kenya's Commitments in Various Regional Treaty Frameworks

By:

Malcolm Kijirah
Elaine Wangari Thuo

May 23, 2022

Various countries, including Kenya have justified the need to control data flows through a multitude of reasons including national security, cybersecurity, personal data protection, data sovereignty, protection of intellectual property, regulation of corporate behavior among others. At a national level, laws on privacy and data protection, which include data localization requirements under

the substantive and procedural laws get their bearing from the Constitution of Kenya, Articles 31(c) and (d) guarantee the right of every person not to have “information relating to their family or private affairs unnecessarily required or revealed and; the right not to have “the privacy of their communications infringed”.

Data localization requirements are laid down under Section 50 of the Data Protection Act 2019 (DPA) and Regulation 25 of the Proposed Data Protection (General) Regulations 2021. Data localization is not defined under the Act but certain restrictions have been introduced with respect to cross-border data transfers. The Act prohibits cross border data transfers unless such transfers are to a country with the same adequate levels of protection as Kenya or approvals have been obtained after the data controller or data processor has given sufficient proof that measures have been put in place to protect the personal data.

There are additional levels of protection for sensitive data. The DPA provides that sensitive data may only be transferred outside the country where the data subject has given express consent, effective and appropriate safeguards have been put in place and in line with the requirements or conditions set by the Data Commissioner.

To operationalize the effect of the DPA, proposed regulations have been introduced which require processing of personal data for the purpose of actualizing a public good, to be done through a server and data center located in Kenya, and at least one serving copy of the concerned personal data is stored in a data center located in Kenya.

At a regional level, while Kenya’s data protection law on cross-border data transfers require that the country where the data is sent to must meet certain conditions such as ensuring safeguards and adequate level of protection in the other country the EAC protocol may be a means of ensuring adequacy status within the community, but such transfer is still problematic to countries outside the community who do not have similar or adequate measures of protection of personal data

To try and resolve this, the Proposed General Regulations in Kenya stipulate that another level of adequacy would be to permit transfer with countries that

are signatory to the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention).

However, despite this proposal, Kenya is not a signatory to this convention. Reciprocal requirements are the norm in many of these treaties, therefore, Kenya's advocacy for the Malabo convention as an adequacy status requirement in the proposed regulations without being a signatory must be addressed by our policy makers.

Kenya must consider these regional treaty frameworks as it settles its data localization laws or risk the loss of opportunities that trading with its partners affords.

Potential Effect of Data Localization Laws in Kenya

Economic Impact

Since data localization may restrict the ability of businesses and individuals from making full use of data, and in effect increase the cost of services that require data, it stands to reason that prices of any goods or services that use data in their production would also increase.

Data localization laws may have a direct impact on various sectors of the Kenyan economy as they may reduce connections to digital trade, stifle innovation, restrict access to new and advanced technology, block competition and add to the cost of maintaining local data infrastructure.

Kenya currently has approximately ten data centers serving a population of approximately 50 million. Given the data localization requirements, more data centers will have to be created which equals increased costs. The cost of maintaining these data center's is exacerbated by massive electricity requirements and reliance on skilled labor that is currently unavailable in Kenya. Thus, it is inevitable that the above costs would be transferred to consumers who are already burdened with the current high cost of living.

Impact on human (Digital) Rights and Freedoms

A country's human rights record poses a credible economic development and reputational risk and affects its economic status, as trade bans and restrictions

are tools used to influence human rights across the globe.

Data localization laws may expose Kenyan citizens to government surveillance, breaches of privacy and cybercrime. On one hand, access to this data allows the law enforcement to investigate and prosecute crime without hindrance, and intelligence services can detect any activity that is contrary to the national security interests. However, this access may easily be misused by government agencies through surveillance of without citizen’s knowledge or consent.

Further storing all the consumer data inside a geographical region may also heighten negative externalities by risking data breaches.

Conclusion

Kenya currently has a unique opportunity to walk the tight rope between considering its national security objectives and the impact restrictive data localization measures will have on its economy, trade objectives and human rights record. A holistic review of sector specific laws providing for data localization requirements is also necessary. The existence of sector specific restrictions may lead to duplicity, failure of compliance due to different standards, as well as establishing a different threshold for protection apart from the one established under the DPA.

Kenya should consider the impact of strict data localization measures on digital trade. Kenya should also sign and ratify the Malabo convention before requiring other countries to do so as a means of meeting the adequacy requirement its data protection regulations proposes. This action will signify Kenya’s commitment to intra-African partnership and will enhance cooperation in the continent. In addition, Kenya should consider concluding reciprocal (bilateral) data protection agreements with specific countries to promote trade as it settles its broader international and regional treaty framework position.

View online: Symposium on the Economic Impacts of Data Localisation in Africa: Data Localisation in Kenya: Potential Economic Impact and Effect on Kenya's Commitments in Various Regional Treaty Frameworks

Provided by Afronomicslaw