Which Way for **Data Localisation** in Africa?

CIPESA

November **2022**

What is Data Localisation?

A growing trend across Africa has been the mandating of data localisation by states. Data localisation refers to the requirement that data about a nation's citizens or residents is initially collected, processed or stored within the boundaries of a particular "jurisdiction", such as a country or a geographic region like a regional economic community or bloc.[1] These restrictions or limitations on data collection, processing, storage or transfer are often stipulated in data protection laws or regulations.

For the most part, rather than institute bans on the cross-border transfer of data, African countries have stipulated conditions under which certain types of data may be exported or processed outside their countries.

Justifications for Data Localisation

There are divergent views on the need and the benefits of data localisation. Proponents often cite the need to protect national security, promote the local digital economy, and to ensure adequate data security and users' privacy.[2] According to them, banning data flows can lead to a loss of jobs, tax revenue, and local capacity in areas such as data hosting infrastructure.

The most basic reason for the increase in data localisation may be traced to the economic value of data. Data is more valuable today than ever before, and perhaps for psychological reasons, but also for practical reasons, countries want to have what is valuable closer to them as it gives them a greater sense of control. At the same time, it is of course true that just having a large stock of data stored locally is not valuable in and of itself. - *Data localisation trends and challenges*

Critics argue that data localisation can undermine data privacy, including by facilitating government agencies' access to their citizens' data, including for purposes of conducting state surveillance. As such, it is contended that "data localisation policies are causing more harm than good" as "they are ineffective at improving security, do little to simplify the regulatory landscape, and are causing economic harms to the markets where they are imposed."[3] According to this school of thought, strengthening state control over users' data "does little to address genuine grievances surrounding cybersecurity, disinformation, or the online targeting of marginalised communities by state and non-state actors."[4]

1 *How Would Data Localization Benefit India? https://carnegieindia.org/2021/04/14/how-would-data-localization-benefit-india-pub-8429*
2 *How Surveillance, Collection of Biometric Data and Limitation of Encryption are Undermining Privacy Rights in Africa, https://tinyurl.com/4ptmxy43*
3 *Emily Wu, Sovereignty and Data Localization, https://www.belfercenter.org/publication/sovereignty-and-data-localization*
4 *Freedom House, User Privacy or Cyber Sovereignty? https://freedomhouse.org/report/special-report/2020/user-privacy-or-cyber-sovereignty*

Moreover, data localisation requirements undermine social, economic and civil rights by eroding the ability of consumers and businesses to benefit from access to knowledge and international markets, and by giving governments greater control over local information.[5] Similarly, data localisation requirements have been identified as a barrier to investment and international trade, as they often require foreign businesses to duplicate infrastructure such as data centres and computing facilities.[6] A further contention is that those forced to abide by data localisation requirements incur considerable cost, such as on local employment and infrastructure investment.[7]

What Informs Data Localisation Regulation Around Africa?

The justifications for data localisation in Africa are not clear. Virtually all the countries that have adopted data localisation requirements without clear explanations. Accordingly, it has been suggested that the increased enactment of data localisation laws in Africa is attributed to the unfounded fears that sending their citizens' data across borders could increase citizens' vulnerability to data privacy and security breaches.[8] However, given the proclivity of many African governments for surveilling their citizens, it is plausible that requiring data to be stored locally is also aimed at enabling easy access to that data by state agencies, including security services.

Flexible data flows guided by common frameworks that are well defined can serve the public good by enabling innovation, jobs creation and e-services development, and facilitating intra-Africa digital trade. As such, there is a need to address policy measures that restrict data flows across borders and mandatory legal requirements that data be stored or processed in a specific country. - CIPESA - Leveraging the African Union Data Policy Framework to Bolster National Data Governance Practices

Which African Countries Have Data Localisation Requirements?

Many African countries have enacted laws that require data to be stored locally and forbid cross-border transfers of personal data unless authorised by the data protection authorities or other designated entities.[9] These include Algeria (article 44 of data protection law, article 10 of ARPCE directive on cloud computing, and the 2018 law on e-commerce); Gabon (article 94 of the Law No. 001/2011 on the protection of personal data); Niger (article 24 of the data protection law); Morocco (articles 43 and 44 of the law No. 09-08 on Processing of Personal Data, 2009); Angola (article 34 of the data protection law); Benin (article 391 of the Benin Digital Code); Burkina Faso (article 42 of the law No. 001-2021 / AN), and Cape Verde (article 19 of the Data Protection Act).

Others include Madagascar (article 20 of the Personal Data Protection Law); Mauritius (section 36 of the Data Protection Act 2017); Lesotho (article 52 of the Data Protection Act 2011); Guinea Conakry (article 28 of the cybersecurity and personal data protection law); Ivory Coast (article 7 of the data protection law); Congo Brazzaville (article 23 of the personal data protection law 2016); Sao Tome & Principe (article 19 of the law on data protection), and Togo (article 28 of the data protection law).

Breaking the Web: Data Localization vs. the Global Internet, https://ssrn.com/abstract=2407858

5 *GSMA, Cross-Border Data Flows_ The impact of data localisation on IoT January 2021,*

6 *https://www.gsma.com/publicpolicy/wp-content/uploads/2021/01/Cross_border_data_flows_the_impact_of_data_localisation_on_IoT_Full_Report.pdf*

Svantesson, D., Data localisation trends and challenges, http://dx.doi.org/10.1787/7fbaed62-en

7 *Data Localization Laws are Making African Trade Less Free, https://weetracker.com/2019/09/20/data-localization-laws-are-making-african-trade-less-free*

8 *CIPESA, Mapping and Analysis of Privacy Laws and Policies in Africa, https://cipesa.org/?wpfb_dl=454*

9

What Data is Subject to Localisation Regulation?

Some *countries use laws* on financial services (e.g. Nigeria, Ethiopia, Rwanda and Uganda), cybersecurity and cybercrimes (Rwanda, Zambia and Zimbabwe), telecommunications (Cameroon, Rwanda and Nigeria), and data protection (Kenya, South Africa, Tunisia and Uganda) to place restrictions on cross-border data transfers.

Various countries have specified the types of data that cannot be exported without authorisation by regulators. Kenya has specified all public data; Nigeria mentions all government data, subscriber and consumer data; while Zimbabwe, Malawi and Tunisia cite "personal information". Sierra Leone's Telecommunications Subscribers Identification and Registration Management Regulations 2020 prohibit the cross-border transfer of subscribers' registration information without approval by the National Telecommunications Commission. Zambia specifies "critical information" in its cybersecurity law, with section 70(2) providing that although the minister may prescribe categories of personal data that may be stored outside the country, "sensitive personal data" is exempted and must be processed and stored in a server or data centre located in Zambia.

A few countries have gone beyond the provisions of personal data protection laws to legislate other data localisation requirements. Morocco requires companies and organisations operating in sectors of "activity of vital importance" and using data deemed sensitive, to host their infrastructure and digital databases on Moroccan territory. Additionally, the National Telecommunications Regulatory Agency requires[10] service providers commercialising the ".ma" domain name to set up and maintain a secure Domain Name System (DNS) service platform made up of at least two DNS servers, including at least one server hosted in Morocco.

Similarly, Algeria requires operators of public cloud computing services to establish their infrastructure on Algerian territory and to host and store their data locally (article 10 of decision No. 48/SP/PC/ARPT/17 of 29 November 2017).[11] Similarly, Algeria requires local e-commerce operators to host their websites in Algeria and with an extension of the ".dz" domain name (article 6 Law No. 18-05 of May 10, 2018 relating to electronic commerce).

Conditions for Cross-Border Transfer

The authorisation requirements for cross-border transfer are similar in most countries. Most conditions require the regulator (mostly the Data Protection Authority, but in some instances the telecoms industry regulator) to allow data export after establishing that the country or organisation to which the data is to be transferred has a similar or higher level of data protection as that of the country of origin of the data. However, there has been *limited recognition* of equivalence in the level of data protection among fellow African countries. For instance, Morocco's 2015 *list* of 32 countries with a sufficient level of protection featured no African country, while Tunisia's 2018 list of *49 countries* had just Algeria, Mauritania, Mauritius, Morocco, and Senegal.

The laws also generally provide similar grounds for when personal data can be sent across borders to a country that does not have an adequate level of data protection. Such transfers may be authorised if the individual has given their consent unambiguously to the proposed transfer, or the transfer is necessary for the performance of a contract between the individual and the data controller, or for law enforcement purposes.

10 *ANRT Morocco, Service provider agreement n ° ../ma/20../ANRT relating to the marketing of ".ma" domain names, https://bit.ly/3c24At4*

11 *Algeria, Decision No. 48/SP/PC/ARPT/17 dated 29 November 2017, https://bit.ly/3F9rKKH*

Enforcement of Data Localisation Regulations

There is limited evidence of how various countries have implemented their legal provisions on data localisation. Data protection bodies created by the countries' respective laws are fairly young, and in some instances, not operational. In others, there is limited evidence as to how - if at all - they enforce the legal provisions relating to cross-border data transfers. As a result there is scant information on enforcement mechanisms, including whether the respective countries are indeed authorising any or all cross-border transfers of the relevant data subject to data localisation requirements.

Similarly, there is scanty information in the public domain on the regulatory sanctions imposed on entities that breach data localisation regulations. A notable exception here is Rwanda, which in 2017 fined telecom operator MTN Rwanda USD 8.2 million for failing to host its data locally. In Morocco, the National Commission for the Protection of Personal Data (CNDP) published a list of countries that offer a sufficient level of protection and comply with the requirements of Moroccan legislation relating to processing of personal data.[12]

Ivory Coast, as an example, has some novel provisions. Notably, article 8 of its data protection law requires controllers to submit to the Telecommunications Regulatory Authority (ARTCI) an annual activity report on the transfer of personal data to third countries. However, there is no evidence that this measure is implemented.

In Benin, before any transfer of personal data is authorised by the Data Protection Commission (CIL), a signed contract must be entered with the third party. The contracts should typically have data confidentiality and data reversibility clauses to facilitate the complete migration of data at the end of the contract. Similarly for Mauritius, under section 36(4) of the data protection law, the Data Protection Commissioner may request a person who transfers data to another country to demonstrate the effectiveness of the safeguards or the existence of compelling legitimate interests and may, in order to protect the rights and fundamental freedoms of data subjects, prohibit, suspend or subject the transfer to such conditions as the Data Commissioner may determine. A similar provision exists under section 48 of Kenya's Data Protection Act, 2019 which stipulates the conditions for the transfer of personal data to another country.[13] In various countries, authorities are yet to enforce these seemingly sound principles.

In many instances, the laws are not clear on the rationale behind the data localisation requirements. Nonetheless, a few have provided justifications, including those related to national security. For example, article 44 of Algeria's 2018 data protection law prohibits any transfer of personal data to a foreign state when it is likely to harm public security or the vital interests of Algeria. Ivory Coast's 2016 law on fighting money laundering and financing of terrorism provides that cross-border data sharing may be prohibited if it infringes the Ivorian sovereignty or national interests as well as security and public order (article 78).

12 CNDP Morocco, Deliberation No. 236-2015 of 2015, https://bit.ly/3C5aKmE

13 Data Protection Act, 2019 http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2024%20of%202019

Enforcing Data Localisation in Rwanda

Rwanda has been positioning itself to become a regional ICT hub and to engender ICT-driven socio-economic development. Data localisation is seen as contributing to this vision of creating local capacity, infrastructure, and jobs. In a directive issued in May 2017, the industry regulator, Rwanda Utilities Regulatory Authority (RURA), faulted MTN Rwanda for failing to shift its data centre from neighbouring Uganda.

At the time, moving the data centre to Rwanda was deemed by some as a complex, expensive and disruptive matter that would undermine the MTN Group's efficient deployment of resources. RURA fined MTN Rwanda FRw 7.03 billion (USD 8.2 million) for breach of the Regulations Governing Telecom Network Security in Rwanda (2016) whose article 16 provided that subscribers' information such as voice, SMS, data including call data records and billing information shall not be transferred, stored or processed outside of Rwanda. The regulator cited article 269 of the law governing ICT, which provides for sanctions against a licensee that fails to comply with a regulatory directive. The sanctions specified in the article include an administrative fine of between FRw 500,000 and 15 million (USD 499-14,960) for each day of non-compliance; imposition of additional conditions on the operator's licence; suspension of a licence for a specified period; and, revocation of a licence.

Enforcing Data Localisation in Tunisia

In November 2017, Tunisia's data protection authority instituted proceedings against OVH Tunisie, a subsidiary of the French cloud computing company OVH on allegations of infractions related to data location.[14] In a lawsuit before the public prosecutor, the National Authority for the Protection of Personal Data (INPDP) said that the company did not disclose to its Tunisian customers where their data was stored nor get their consent. Furthermore, the regulator alleged that the OVH transferred data from Tunisian customers abroad without requesting authorisation from the INPDP, in violation of article 52 of the data protection law.

Uganda: When Security Agencies Gain Unauthorised Access to Telecom Users' Data

In July 2018, Ugandan *security agents* from the Internal Security Organisation (ISO) *stormed* the Data Centre of leading telecom service provider MTN Uganda without a search warrant, a court order or request for information served to the telco, and reportedly accessed confidential data, including call data records.[15] There were unconfirmed *reports* that the security agents were investigating MTN Uganda for rendering assistance to Rwandan intelligence to spy on Ugandans at a time when the two countries were trading accusations of supporting each other's enemies.

In a complaint to the regulator, MTN Uganda stated that the incident posed a serious security risk to its telecommunications infrastructure and customer data, adding that "ït is possible some data may have been tampered with or illegally accessed and taken from the premises."[16] Uganda's laws, including the Computer Misuse Act, permit police officers access to users' data particularly if their requests are backed by a court order. With or without court backing, however, it is easier for overbearing security agencies to access locally stored data than data stored abroad.

14 *INPDP Report https://thd.tn/linpdp-apporte-des-precisions-sur-laffaire-dovh-tunisie*

15 *Nobody is above the law! ISO boss justifies raid on MTN data centre, https://www.pmldaily.com/news/2018/07/nobody-is-above-the-law-iso-boss-justifies-raid-on-mtn-data-centre.html*

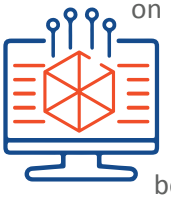
16 *MTN Uganda says government security personnel raided its data center, https://www.reuters.com/article/us-uganda-mtn-group-idUSKBN1JW1Q5*

17 *Computer Misuse Act https://ulii.org/akn/ug/act/2011/2/eng@2011-02-14#part_V__sec_28*

Data Localisation and Regional Instruments

The various African data localisation mandates appear to contradict continental initiatives such as the Policy and Regulation Initiative for Africa (PRIDA) and the African Continental Free Trade Area (AfCFTA), which are premised on flow of data across borders. Below, is what some regional instruments stipulate on data localisation.

The 2019 Declaration of Principles of Freedom of Expression and Access to Information in Africa, of the African Commission for Human and Peoples' Rights (ACHPR), under Principle 40(3) provides that states shall not adopt laws or other measures prohibiting or weakening encryption, including backdoors, key escrows and data localisation requirements, unless such measures are justifiable and compatible with international human rights law. Moreover, Principle 42(4) of the ACHPR Declaration provides that "Every person shall have the right to exercise autonomy in relation to their personal information by law and to obtain and reuse their personal information, across multiple services, by moving, copying or transferring it."



The African Union (AU) Data Policy Framework of 2022, in a situational analysis of the data economy on the continent, identifies one of the weaknesses as "localisation rules that limit the cross border flow of information necessary for local value creation and establishment of the single market." It calls for intensification of international cooperation on cross-border data flows to ensure that data localisation requirements and other restrictions on cross-border data flow do not unduly interfere with cross-border communications and the economic and societal benefits that global data networks make possible and are minimally trade-restrictive, while promoting trust.

The Digital Transformation Strategy for Africa (2020-2030): Among the objectives to drive digital transformation in the AU to propel industrialisation, contribute to the digital economy and support the African Continental Free Trade Area (AfCFTA), is to "promote open standards and interoperability for cross-border trust framework, personal data protection and privacy." Further, the Strategy calls for harmonisation of policies, legislation and regulations related to digital networks and services, intra-Africa trade, intra-investment and capital flows.

The *African Union Convention on Cyber Security and Personal Data Protection* provides a legal framework for cyber security and personal data protection for African Union Member States. Article 10 provides for preliminary personal data processing formalities. Article 10(6) provides that requests for opinion, declarations and applications for authorisation shall, among others, indicate envisaged transfer of personal data to a third country that is not a member of the African Union, subject to reciprocity. Article 12 on duties and powers of national protection authorities includes authorising trans-border transfer of personal data. The Specific principles for the processing of sensitive data in article 14(6)(a) also prohibit transfer of 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 b e processed.

Which Way For Data Localisation in Africa?

Evidence is thin on the data security practices for locally hosted data in countries with local data residency regulations, and the impact it has had on enhancing or curtailing citizens' privacy rights. Notably, the growing appetite for state surveillance could be a key driver towards the adoption of data localisation laws. Hosting data locally could thus grant state surveillance apparatus in *some countries* in the region easier access to data for surveillance purposes, as they would not need to go through foreign countries' or intermediaries' data management protocols to access this data.

On the other hand, hosting data locally may enable and drive local innovation and spur investments in local ICT and hosting infrastructure if the right incentives for investment, the requisite skills, and enabling provisions on access to data and data use and reuse, are in place. However, it should be realised that not all African countries have the technological capacity or infrastructure, such as data centres, to meet the localisation demands mandated by their privacy laws.

Recommendations

- Balance between data localisation and privacy by putting in place strong legal and policy measures for data protection to prevent any cases of overlaps that would unnecessarily lead to data breaches.
- Institute all necessary measures to ensure that they take advantage of cross-border data flows in an increasingly digitalised, globalised and integrated world, including by growing local capacity to use and reuse data.
- Generate evidence that addresses the fears that inform states' restrictive regulatory stances on cross-border data transfers.
- Move faster towards policy harmonisation across African countries using the Malabo Convention, among other regional instruments, as a blueprint to improve data flows across countries while ensuring data privacy.
- Comply with duties and obligations under article 9 of the African Charter on the right to receive information and free expression, as supplemented by Principle 40(3) of the ACHPR Declaration which provides that "states shall not adopt laws or other measures that prohibit or weaken encryption or that impose data localisation requirements."

CIPESA

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)

+256 414 289 502

programmes@cipesa.org

@cipesaug facebook.com/cipesaug Linkedin/cipesa

www.cipesa.org