THE IMPORTANCE OF DATA LOCALISATION IN CYBERCRIME INVESTIGATIONS

AFRICAN DATA PROTECTION LAWS: REGULATION, PRACTICE AND POLICY CONFERENCE

13 – 15 SEPTEMBER 2022

UNIVERSITY OF GHANA, ACCRA

Melody Musoni

INTRODUCTION

In the global and interconnected world, data are indispensable. Importantly, the sharing of data between service providers and customers in different countries is the backbone of international trade. The COVID-19 pandemic facilitated the growth in digital trade and cross border data flows even when global GDP growth rates plummeted. Data generates a lot of value for governments, the digital economy, and individuals. The United Nations estimate that by 2025, 49% of data will be stored in the cloud. Cloud computing technologies play a central role in the processing and storage of this data.

While data are crucial for the digital economy, they also play an important role in cybercrime investigations. There is an increase in the requirement for crime investigators to access electronic evidence stored in the cloud. However, features of cloud data such as data fragmentation, divisibility, encryption, mobility and location independence can present jurisdictional challenges for cybercrime investigations. International criminal law on enforcement jurisdiction limits the powers of law enforcement agents when conducting searches and seizures of data hosted in foreign territory. When data are hosted on servers in foreign territory, law enforcement agents need to obtain the necessary authorisations from the foreign state before they can exercise any enforcement powers over the data.

To avoid these hurdles as well as other policy concerns such as national security interests and protection of citizens' privacy, states are resorting to implementing data localisation measures. With data localisation measures, data or copies of data becomes easily accessible by law enforcement exercising their enforcement powers. This presentation seeks to highlight the role played by data localisation measures in solving the challenge for law enforcement agents accessing remote evidence.

OUTLINE

What is data localisation?

Why do African governments enforce data localisation measures?

Is there a justifiable link between data localisation and effective cybercrime investigations on the African continent?

What are the recommendations for effective cybercrime investigations and prosecutions and promotion of cross border data flows?

WHAT IS DATA LOCALISATION?

WHAT IS DATA LOCALISATION?

There is no official definition of data localisation. Fraser defines data localisation as the laws or measures put in place by governments which encumber the movement of data across national borders or limit where and by whom they are stored or processed (*Erica Fraser*).

It is an explicit requirement that data be stored and / or processed within the domestic territory (*Gonzalez, Casalini and Porras*). Data localisation mandates come in different forms or manifestations which also determine the definition of the term.

Some consider it as a second generation internet border control (*Anupam Chander*). It involves the artificial erection of legislative barriers to data flows, such as through data residency requirements and compulsory local data storage (*AU Data Policy Framework*).

FORMS OF DATA LOCALISATION MEASURES

Soft localisation

- No restrictions on data transfers
- Copy of data may be stored locally
- Alternatively, firms should guarantee access to data when requested

Conditional localisation

- Measures that mandate local storage of data
- Allow transfer or processing abroad under clearly defined conditions
- Some data protection laws and conditions on cross border data flows may result in de facto localisation

The GDPR does not have explicit data localisation clauses, but the effect of its conditional transfer can result in de facto data localisation (OECD Trade Policy Paper, 2022) (Sheppard, Yayboke and Ramos 2021).

Strict localisation

- Mandatory local storage of data and prohibitions on cross border data transfers.
- It could be a blanket ban on all data transfers or ban on specific industry sectors like finance or health

DATA LOCALISATION ON THE AFRICAN CONTINENT

DATA CENTRE CONCENTRATION ON THE AFRICAN CONTINENT

The cloud is becoming the lifeblood of the African economy and there are great prospects for cloud computing to flourish in the 4IR. Main data centres in Africa - Kenya (5); Nigeria (11); Morocco (5); South Africa (25). However, the majority of data centres and cloud services are offered or under the control of foreign entities. Foreign owned companies (from the USA (GAFAM) or China (BATX - Baidu, Alibaba, Tencent and Xiaomi)) have been in action for building their cloud services on the continent.

- ✓ Microsoft has launched enterprise grade data centres in South Africa and edge nodes in Kenya, Nigeria and Egypt.
- ✓ A US entity acquired a stake in Teraco which owns Africa's largest data centres.
- ✓ Actis launched pan-African data centres in countries like Nigeria.
- ✓ Africa Infrastructure Investment Managers private equity firm acquired a majority of stake in Ngoya Etix DC, a carrier-neutral data centre located in Ghana.
- ✓ Liquid Intelligent Technologies recorded an influx in investor interest including from the US government's International Development Finance Corporation.

(*Africa Digital Infrastructure Market Analysis 2021 Report*).

What does foreign control over African data and data centre infrastructure mean for Africa?

'*An increasingly common way for a nation to assert data sovereignty, particularly if the country is not in a dominant position of geopolitical power is to pass data localisation measures*'

WHY IS DATA LOCALISATION EMERGING ON THE AFRICAN CONTINENT?

Africa has witnessed a growing number of laws and policies which promote data localisation. The approaches to data localisation depend on a state's policy objectives. Governments' power is diminishing due to the growth in market share by major multinational tech companies. Technology companies exercise monopoly over data which allows them to capture political power, determine the level of their involvement in how the data are used. African governments are also concerned about data colonisation (*Nima Elmi, 2020; Nigel Cory and Luke Dascoli, 2021*).

African governments believe that data localisation requirements will help them re-gain their data sovereignty and have autonomy to decide for themselves how to regulate their digital infrastructure and how to plan their digital futures (*African Union Data Policy Framework 2022*).

In cybercrime investigations, tech companies play a pivotal role. Law enforcement rely on their technical assistance when seeking access to cloud evidence. It is up to the service providers to provide access to sought after evidence or resist the requests. These companies exercise discretion over who may get access to customer data. The role of governments has both been supplemented and sometimes supplanted by these private actors (*Jennifer Daskal*). When companies refuse to cooperate or disclose data, this threatens the sovereignty of a state (*Matthew C Snipp*).

WHY IS DATA LOCALISATION EMERGING ON THE AFRICAN CONTINENT?

The concern is that if states are not careful on the amount of influence and authority exerted by service providers, their powers are likely to wane off. To exert their sovereignty over data, states may resort to data localisation measures (*Jennifer Daskal;* *South Africa draft National Cloud and Data Policy*). Apart from establishing data sovereignty or digital sovereignty, African governments also adopt data localisation measures for the following reasons:

Citizens' privacy and security reasons - When data are stored abroad, there are legitimate concerns relating to the privacy interests of the owners of the data. There are concerns that many organisations which collect, process and store massive amounts of data lack security and privacy protections. This argument emanates from the lack of robust data protection laws in other jurisdictions. Absence of effective data protection laws means that foreign based data can easily be accessed by foreign governments.

National security interests - Some countries view localisation as critical to protecting their respective citizens from foreign covert surveillance mainly from the United States government. What the revelations made by Edward Snowden highlight is that the United States of America carries out mass surveillance on foreign governments and foreign citizens. It is argued that data localisation prevents or protect data from access by distrusted agents or governments. Zimbabwe, Zambia, Rwanda have adopted laws to protect national security interests.

Protection of domestic businesses - to help develop domestic capacity in digitally intensive sectors. Nigeria has introduced data localisation measures to protect domestic companies operating in the ICT sector.

POLICY AND LEGISLATIVE CONTEXT ON DATA LOCALISATION ON THE AFRICAN CONTINENT

- The AU Data Policy Framework

It is an effort by African governments to consolidate the data environment and harmonise digital data governance systems to enable the free and secure flow of data across the continent while safeguarding human rights, upholding security and ensuring equitable access and sharing of benefits. The Policy Framework reiterates that cross border provisions for cloud computing services and data centres such as data privacy, security and restrictions on where data are housed (localisation requirements) need to be decided in consideration of broader economic development priorities. The Policy Framework highlights the importance of a cost-benefit assessment prior to adoption of data localisation measures. It points out that localisation needs to be evaluated against potential harm to human rights.

There are other frameworks which addresses aspects of data localisation and cross border data flows

- African Union Convention on Cyber Security and Personal Data Protection
- The African Commission on Human and People's Rights Declaration of Principles of Freedom of Expression and Access to Information
- Digital Transformation Strategy for Africa 2020-2030
- The African Continental Free Trade Agreement
- Regional Model Laws on Data Protection - 2008 East African Community Framework for Cyberlaws / 2010 Supplementary Act on Personal Data Protection of the Economic Community of West African States / 2013 SADC Model Law on Data Protection

AFRICAN COUNTRIES' APPROACH TO DATA LOCALISATION

South Africa - The draft National Data and Cloud Policy; The Protection of Personal Information Act 4 of 2013; 2014 South African Reserve Bank Guidance Note Outsourcing of Functions within Banks; 2018 Cloud Computing and Offshoring of Data Directive.

The draft National Data and Cloud Policy notes that South Africa and Africa are unequal participants in the cloud market when compared to North America, Europe, and Asia. It identified important policy concerns which justifies the adoption of data localisation measures. South Africa is not competitively participating in data centre infrastructure. First, the cloud market is dominated by foreign owned companies who are providing local cloud services. Secondly, a significant amount of data of South African businesses, citizens, residents, and government departments is being hosted on foreign based data centres. South Africa recognises that data ownership, data sovereignty and data protection are critical elements for the digital economy and seeks to put in place measures to decentralise investments to ensure distribution of opportunities in the cloud computing area. South Africa's draft National Data and Cloud Policy provides that data generated in South Africa is the property of South Africa, regardless of where the technology company is domiciled. The policy also clarifies that data generated by foreign tech companies also belongs to the South African government.

South African Reserve Bank Directive and Guidance Note require banks to notify the Office of the Registrar of Banks before offshoring material IT business. Banks must notify the Reserve Bank of any outsourcing arrangements, like cloud contracts, which they intend entering which have a bearing on the risk profile of the bank, affects the systems and controls of the bank, is classified by the bank's management as being of strategic importance and which has implications for the Reserve Bank's discharge of its supervisory responsibilities.

AFRICAN COUNTRIES' APPROACH TO DATA LOCALISATION

Ethiopia

Licensing and Authorisation of Payment System Operators Directive No. ONPS/02/2020, the transfer of domestic payment information outside of Ethiopia for the purposes of authorisation, clearing and settlement by Point of Sale (POS) machine operators is outlawed. ATM operators are prohibited from sending any transaction data outside Ethiopia for processing, authorisation and switching.

Nigeria

NITDA require telecommunication and networking services companies to host all subscriber and consumer data within the country; Central Bank of Nigeria's 2011 Guidelines on Point of Sale Card Acceptance Services requires entities engaging in POS services to use a local network switch (which connects devices and processes information to and from connected devices) for all domestic transactions. Domestic transactions cannot be routed outside Nigeria for switching between Nigerian issuers and acquirers.

Rwanda

Protection of Personal Data and Privacy Law 058/2021 (Art 48); Regulation No. 02/2018 on Cybersecurity provides that any bank licensed by the Central Bank must maintain its primary data within the territory of the Republic of Rwanda (Art 3). Article 27 of the 2010 law governing the credit information system in Rwanda provides that the Central Bank shall have the authority to approve the sharing of customer information beyond the borders of Rwanda.

THE ROLE OF DATA LOCALISATION IN CYBERCRIME INVESTIGATIONS

CLOUD DATA AND ENFORCEMENT JURISDICTION

What are the features of cloud computing technologies

How do cloud features affect the exercise of enforcement jurisdiction?

- Data may be hosted on servers located in foreign territory.
- Data may be hosted on servers in multiple jurisdictions.
- Data may be in transit which means that there is a loss of knowledge of location of data at a particular time.
- Data may be encrypted making it difficult for law enforcement to determine if they have jurisdiction over the data.

DATA DIVISIBILITY, FRAGMENTATION & IMPACT ON JURISDICTION

The distributed, dynamic and redundant nature of cloud storage makes it difficult to say 'where' a certain file 'is' when it is stored in the cloud. This is because it can be in multiple places simultaneously and still not be in any single place in its entirety. If data are divided and randomly scattered on data servers around the world, the challenge becomes which states will exercise jurisdiction over the cloud data. States where the data are located can exercise jurisdiction over the cloud data. If the data are hosted in servers in multiple states, the data are subjected to different laws and be subject to simultaneous seizure by multiple different law enforcement agencies.

When data are localised, law enforcement can easily access copies of data as it is within their territorial jurisdiction.

DATA MOBILITY, TRANSIT DATA AND JURISDICTION

One of the principles of information security is maintaining copies of data on replica data centres. Most cloud service providers operate replica data centres. Data algorithms constantly move replicated or fragmented data around different servers within or across different countries at any time. When data are in transit, its location may be difficult to ascertain. What this means for law enforcement agents is that they cannot get a search warrant from court, as the location of the evidence requirement cannot be met. This can be a constant hurdle for law enforcement agents since data are constantly moved around different servers for efficiency and improving availability.

If the location of data is unknown, law enforcement agents cannot blindly conduct searches and seizures. To do so would likely threaten the sovereign interests of a foreign state, where the sought-after data happen to be located. Without knowledge of location of data, mutual legal assistance may not be feasible. The investigating state will not know which country to approach for legal assistance and cooperation.

LOCATION INDEPENDENCE & JURISDICTION

Location independence mean that cloud data can be accessed from an arbitrary location.

If data could be accessed and manipulated remotely, should law enforcement agents unilaterally access the data?

The challenge with data residency is that a foreign state may have a stronger jurisdictional basis over cloud data. The basis of jurisdiction could be because the data centres are established within that state or alternatively the cloud service provider is registered within that state. An investigating state may not always have a stronger basis to exercise jurisdiction over cloud data even in cases where the crime was committed by a citizen and within its borders. If the investigating state and the foreign state do not have good diplomatic relations for the exercise of mutual legal assistance, the investigating state can potentially resort to unilateral access to cloud data.

Cloud services are a remote service offering which means that the cloud service provider does not necessarily have to establish a legal presence in every jurisdiction. Most cloud service providers on the African continent have no offices in countries where they are offering services. Without a legal presence, law enforcement agents in Africa may find it difficult to force the foreign service providers for their assistance in an investigation.

Due to location independence of cloud data, states are concerned that cloud service providers will escape regulation and other legal responsibilities simply because they are not territorially located there. This is one of the challenges that law enforcement agents may face when seeking to compel the service provider to disclose or produce cloud data of persons of interest (*Jennifer Daskal*).

LIMITATIONS OF MUTUAL COOPERATION

Data hosted on foreign data centres are subject to the laws of the foreign state where data centres are located (cross border data are extraterritorial). To comply with international law, foreign law enforcement seeking cloud evidence on foreign servers need to follow the available channels for assistance instead of acting unilaterally. One of the common ways to access the data is getting permission through the mutual legal assistance treaty (MLAT) channels.

If mutual cooperation processes are in place, why insist on data localisation measures?

Slow processes. For instance, the US government can take up to 10 months to complete MLAT requests (leading to a massive backlog), while requests from the US to Ireland take only 15 to 18 months. Meanwhile some countries take years to respond to requests, while others, such as Russia, often do not respond at all.

The danger with snail-paced processes is they are likely to result in miscarriage of justice as criminals may get rid of evidence while an investigating state is still waiting for approval from the foreign state. In instances where data are in transit, the service provider may not have knowledge of the location of data. This will make it difficult for the investigating state to identify the foreign state with jurisdiction at that given moment. This could potentially delay the process of gathering evidence.

CONFLICT OF LAWS OVER CLOUD DATA

Cross border data may also be subject to conflicting laws of different states. Compelling service providers to disclose data may be unreliable in instances where laws of the state where the data are hosted do not permit disclosure. This will likely make crime investigation for a state a cumbersome process. However, if copies of the same data were to be locally stored, it is easier for an investigating state to exercise enforcement jurisdiction over locally stored cloud data. Data localisation therefore makes the processes of gathering electronic evidence for criminal investigations fast and efficient.

Local data means that law enforcement authorities will have territorial jurisdiction over the cloud data. Secondly, law enforcement save time and resources by not having to go through the MLAT processes. Thirdly, territorial jurisdiction reduces the friction with companies and service providers as they cannot dispute the jurisdictional authority of the law enforcement. Fourthly, service providers will not be able to rely on excuses such as data being in transit and thus not certain whether the state has jurisdiction, as copies of the same data will be required to be stored locally (*Andrew Woods*).

RECOMMENDATIONS

IMPROVEMENTS IN MUTUAL COOPERATION

Cooperation among states remains the founding basis for any viable solution to data jurisdiction, criminal investigations and successful criminal prosecutions especially for cybercrime. There are several international covenants which promote cooperation between states for purposes of criminal investigations. Lack of mutual understanding by countries may result in the proposed framework being futile. States can only be efficient in processing large numbers of requests for electronic evidence if they receive mutual assistance from other states. Cooperation among governments remain as one of the pillars for effective cybercrime prosecution at a global level. To respect the sovereign interests of other states, states should deal with jurisdictional questions through a series of bilateral or multilateral agreements.

Mutual cooperation starts with states reaching consensus on important aspects relating to transborder data. The type of data sought can be used as a determining factor on whether the investigating state should obtain permission from the foreign state. This is made possible by the cooperation and mutual understanding among states on which type of data requires direct access and which types of data requires indirect access.

IMPROVEMENTS IN MUTUAL COOPERATION – MALABO CONVENTION

African regional cooperation

Mutual cooperation on the African continent starts with the operation of the Malabo Convention. 13 countries have already ratified the convention and signatures of two countries required before the treaty comes into force. Ratification and operationalisation of the Malabo Convention means access to data (on the continent) by law enforcement will be easily facilitated.

Most cloud service providers choose data centres in South Africa, Kenya and Nigeria for storage of African data due to latency.

The Malabo Convention does not provide broad cooperation among African Union members, but this is a stepping stone towards promoting cooperation among African states during cybercrime investigations.

IMPROVEMENTS IN MUTUAL COOPERATION – BUDAPEST CONVENTION

Budapest Convention and the 2nd Additional Protocol

Article 18 of the Budapest Convention

The 2nd Additional Protocol to the Convention on Cybercrime provides for measures for enhanced cooperation and provide a more streamlined mechanism for issuing orders or requests to service providers in other state parties to provide data.

Procedures enhancing direct cooperation with providers and entities in other Parties (Domain name registration information) and (Subscriber information)

Procedures enhancing cooperation between the authorities (Traffic data and subscriber information); (Stored computer data in cases of emergency); (Emergency mutual assistance)

Procedures pertaining to international cooperation in the absence of applicable international agreements (Video conferencing) and (Joint investigation teams and joint investigations)

Some African countries have ratified or acceded the Budapest Convention – Benin, Burkina Faso, Cape Verde, Cote d'Ivoire, Ghana, Mauritius, Morocco, Niger, Nigeria, Senegal and Tunisia. The transfer or sharing of evidence under the 2nd protocol which consists of personal data must comply with applicable data protection agreements or arrangements. To benefit from the Budapest Convention and the 2nd Protocol, African countries need to make sure there are effective data protection laws in place to protect and safeguard personal data which may be the subject of an investigation.

African countries can only benefit from the Budapest Convention and the 2nd Additional Protocol if they have adequate data protection laws and implement acceptable data protection practices.

MULTI-STAKEHOLDER APPROACH BEFORE ADOPTING DATA LOCALISATION MEASURES

When it comes to safeguarding the privacy interests and security of data, governments are usually not the primary actors as that role falls on service providers. Service providers are also central to investigations as the bulk of sought-after data are under their control or possession. Decisions of private actors often determine which government's rules apply, how these rules are interpreted, and how much of data are and should be accessible to governments.

Unfortunately, the global cybercrime legislative landscape reflects a multilateral model. Under this model, countries exercise cyber sovereignty by formulating the rules that apply in cyberspace based on their sovereignty over the territory or the persons involved. Innovative governance means replacing the multilateral model with the multi-stakeholder approach. The multistakeholder model of internet governance is the best mechanism for maintaining an open, resilient, and secure internet because, among other things, it is informed by a broad foundation of interested parties, including businesses, technical experts, civil society, and governments arriving at consensus through a bottom-up process regarding policies affecting the underlying functioning of the internet domain system.

If a multi-stakeholder approach is adopted and all interested players are engaged in the discussion, solutions better than data localisation can be presented and jurisdictional terms of service may be drafted which balances the needs and rights of individuals, service providers, governments, civil society and overall public interest.

A UNITED NATIONS TREATY ON CYBERCRIME

Adopting a more global framework on cybercrime through the United Nations is very important in resolving a lot of jurisdictional challenges to accessing cross border data. (*Schjolberg and Ghernaouti-Helie*). Such a global framework should include the necessary jurisdictional provisions in terms of international law. Jurisdictional provisions would relate to serious crimes in cyberspace whether or not they were possible to prosecute under national law. Currently, the United Nations is considering a UN treaty on cybercrime. While the Budapest Convention has been viewed as an important instrument, it is limited as it is not open for signature to every state. A UN treaty is more likely to provide universal approach to issues around cross border cloud data, thus limiting the requirements for localisation of data for law enforcement purposes.

EXECUTIVE AGREEMENTS

African countries should consider new legal mechanisms that make the exchange of data for law enforcement purposes more efficient while still providing privacy and other safeguards. African states need to be strategic – if the majority of service providers are foreign-owned entities and data are hosted on foreign territory, strive to conclude executive agreements with the governments from where the entities are based. CLOUD Act Executive Agreements as an example.

The CLOUD Act permits the United States to enter into Executive Agreements with a qualifying state. If there is an Executive Agreement in place, law enforcement agents can directly approach the service provider to disclose data. An Executive Agreement is only concluded if it can be shown that the domestic law of the foreign government affords robust substantive and procedural protections for privacy and civil liberties considering the data collection and activities of the foreign government that will be subject to the agreement. The submission must also show that the foreign government has adequate substantive and procedural laws on cybercrime and electronic evidence as demonstrated by being a party to the Cybercrime Convention.

CONCLUSION

Implementing strict data localisation measures as a response to the challenges with exercising enforcement jurisdiction over cross border data should be discouraged. While there are justifications for requesting service providers to keep copies of data on local servers, there are other effective measures which can assist in cybercrime investigations.

First, African countries need to take steps to **promulgate laws on cybercrime which also make provision for providing assistance to foreign law enforcement agencies investigating crime**.

Second, African governments **must ratify the Malabo Convention as it is an important framework to facilitate cooperation among African states.**

Third, countries must **improve their mutual legal assistance channels by reducing the turnaround times to respond to a request, and making it possible for foreign states to directly approach service providers for access to cloud evidence**.

Fourth, governments should **refrain from regulating digital spaces and imposing measures such as data localisation requirements without engaging with relevant stakeholders**.

Fifth, before adopting any strict data localisation measures, governments need to get an **analytical and empirical handle on the twin problems of data localisation and barriers** – not only their scope and impact, but also their root causes and the design of governance mechanisms that could help mitigate their negative effects (*William J Drake*).

THANK YOU

MELODY MUSONI

MELOMUSONI@GMAIL.COM