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

Hanani Hlomani
and
Caroline B. Ncube

Working Paper DG-004

AFRICAN ECONOMIC RESEARCH CONSORTIUM
CONSORTIUM POUR LA RECHERCHE ÉCONOMIQUE EN AFRIQUE

Bringing Rigour and Evidence to Economic Policy Making in Africa

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

By

Hanani Hlomani
University of Cape Town

and

Caroline B. Ncube
University of Cape Town[1]

AERC Working Paper DG-004
African Economic Research Consortium, Nairobi
February 2023

THIS RESEARCH STUDY was supported by a grant from the African Economic Research Consortium. The findings, opinions and recommendations are those of the author, however, and do not necessarily reflect the views of the Consortium, its individual members or the AERC Secretariat.

Published by: The African Economic Research Consortium
P.O. Box 62882 - City Square
Nairobi 00200, Kenya

Contents

Abstract

In a broad sense, this paper seeks to address the concerns associated with data regulation on the African continent. In particular, the paper zooms in on three major aspects of data regulation 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. This will be in the general context of Africa, with a focus on regulatory instruments from the different bodies at continental and sub-regional level, and 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 European Union, 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 African Continental Free Trade Area, and an enhanced digital economy as motivated for in the Digital Transformation Strategy for Africa (2020-2030).

Keywords: *Data; Data Governance; Data protection; Personal Data; Non-Personal Data; Open Data; Cyber-Security; Development; Africa; Malabo; AfCFTA*

1. Introduction

Fast-paced technological advancements have made it difficult for legal scholars, policy makers and legislators to stay abreast of all the considerations and important policy debates that are necessary to ensure that the law is not outpaced and eventually invalidated by technology. The period 2019-2020 evidenced that it is possible for the world to move to a partially or fully digitized eco-system. It has already been said that several global corporations are contemplating whether reverting to the old way of working in the post-COVID-19 pandemic period would make sense given how efficiently the world has been able to adapt, collaborate and produce results in a digital ecosystem. At the centre of it all has been the need to move data from device to device, from one location to another and from one person to the next. This creates a legal conundrum for those tasked with legislating and policy making, who have the task of formulating sound policies and legislative instruments that ensure that such data can move freely, lawfully and without impeding on any personal or commercial interests in a safe digital environment that is protected against cyber-attacks.

Data can be defined as pieces of information that can either be qualitative or quantitative.[2] Such information can be abstract or about one or more persons.[3] Data can also be defined as a collection of facts such as words, numbers or observations or a way of describing things.[4] The term 'data' is not to be confused or used interchangeably with the term 'information.' This is because data is a collection of facts that are unstructured and unorganized whereas information relates to how one understands those unorganized facts contextually.[5] Because of the nature of the digital ecosystem, which is heavily reliant on decentralization, data has been coined as the 'new frontier for economy' after gold (Manzo, 2019). This is principally because data is the means through which devices communicate with one another and the main asset on which markets, research, governments and corporate companies rely daily.[6] Given the decentralization of modes of communication and the flood in web connectivity, a lot of data is exchanged amongst users of the Internet and may include information ranging from personal details of people to anything in between of a non-personal nature.[7] As more data becomes available and accessible, the practice of data analytics becomes increasingly important. Data analytics is a process that uses advanced analytic techniques such as predictive analysis, statistical analysis and data mining on sets of data to discover new facts, to predict future events or behaviours or to explain past phenomena that previously had no logical explanations (Russom, 2013). Such

analytic techniques have the potential to positively impact a number of economic sectors across the African continent, mostly by equipping various stakeholders with information that they previously did not have and from a wealth of resources that were previously blocked by legislation or as a result of geographical barriers.

Currently, debates around data regulation hinge on whether the data in question is personal or non-personal because of the starting premise that from a regulatory approach, personal and non-personal data should not be subjected to the same scrutiny. Personal data can be defined as any information related to an identified or identifiable natural person.[8] This means that a data subject is identifiable if it is possible to directly/indirectly identify the subject through identifiers such as name, identification number, location data, physical, genetic data, cultural data etc.[9] Practically, this can also include all data which are or can be assigned to a person, such as the telephone, credit card or personnel numbers of a person.[10] The opposite, and therefore the definition of non-personal data is electronic data that does not contain any information that can be used to identify a natural person. Examples include data that is non-personal to begin with, for example weather data, stock prices, etc or it can be data that was previously personal in nature but has become anonymized (void of all personal data).[11]

As has been stated, the rate at which technology is advancing makes it increasingly difficult to keep up with how best to regulate data. The African continent has seemed to be more concerned with the protection of personal data of its citizens. It is estimated that approximately 24 of Africa's 55 countries have enacted or embraced some form of regulation, with the aim of protecting personal data.[12] This has largely been attributed to the enactment of the European General Data Protection Regulation (GDPR),[13] which was adopted in 2016 and is very influential due to its regulation of cross-border data flows, and which has impacted a number of countries data protection models globally. However, most innovation-driven countries have realized the value in formulating regulatory regimes that protect personal data while ensuring, at the same time, that non-personal data can be extracted from personal data so that innovation is fostered. In other words, in addition to the value of naturally non-personal data, there is also value in data that was locked away in datasets that have personally identifiable information.

Current African States' approaches and significance for the African Continental Free Trade Area

The African Union (AU) in 2014 adopted the Convention on Cyber Security and Personal Data Protection at the Twenty-third Ordinary Session of the Assembly, held in Malabo, Equatorial Guinea (known as the Malabo Convention), which has not yet come into force because the required number of ratifications has not been reached. This convention, much like the GDPR, focused on personal data and cyber security.[14] At the time of writing (October 2021), the AU Commission is formulating the Africa Data

Policy Framework, which is informed, in part, by the Malabo Convention.[15] Several regional economic communities (RECs) have also adopted regulatory instruments, which will be summarized in section 3. Outside of this concerted effort, very little has been done in terms of a collective continental/regional legislative instrument on data protection, with most countries opting to attempt protection individually.

As the continent moves to realize the promises of the African Continental Free Trade Area (AfCFTA), it will be important to have a measure of harmonization in regulatory frameworks so that inter-Africa trade is enhanced. Businesses and individual entrepreneurs trading in different countries across Africa would benefit if they had some assurance that similar principles of data protection and data governance models are aligned across the continent. E-commerce and digital trade grew exponentially during the last two years due to restrictions on physical interactions between persons to curb the spread of the COVID-19 pandemic. The AU is spearheading the growth of digital trade through the Digital Transformation Strategy for Africa 2020–2030[16] and in this context, an e-commerce protocol is being negotiated under the AfCFTA agreement.[17] It is envisaged that the AfCFTA and the Digital Transformation Strategy for Africa will catapult Africa's digital economy (Chaytor, 2020). As elaborated in section 3, the free movement of data is a core element of promoting inter-Africa trade and cross-border data flows to bring significant benefits. Beyond the AfCFTA e-commerce protocol negotiations, there is global momentum on similar negotiations. Specifically, the World Trade Organization (WTO) began negotiations on trade-related aspects of e-commerce in January 2019, and these are continuing.[18] The development of common African approaches will therefore be instrumental in shaping the global WTO agenda (Okonjo-Iweala, 2021).

Defining personal data

Demarcating what falls within the boundaries of personal data has befuddled scholars for a while. While obvious data such as names, ID numbers, etc are unmistakably personal data, the EU's definition of personal data in Article 4.1 of the GDPR defines personal data as any information-related to an identified or identifiable natural person. Since the definition includes "any information," one must assume that the term "personal data" should be as broadly interpreted as possible. It is for this reason that the bounds of what data is personal or not are constantly being debated.

In the *Breyer* case,[19] the Court of Justice of the European Union (CJEU) in attempting to define what "personal data" is, held that any piece of information, that when additional information is sought from a third party, is able to identify a data subject shall constitute personal data.[20] As such, if one were to apply the principles of *Breyer* practically, the likelihood of data, which initially presented itself as non-personal data, may eventually fall within the ambit of the GDPR's definition of personal data.[21] As that is the case, failing to account for non-personal data may mean that it is subjected to the same restrictions as personal data or other data localization requirements.

In addition to the blurred lines on what constitutes personal data, data localization requirements also pose a threat to radical economic transformation on the African continent on the back of the data revolution. Data localization requirements are typically restrictions on the flow of data from one country to another. For example, it may be required by law that all processing of data relating to a certain country's citizens be carried out using servers located within such a country's borders, and thus making it illegal to process such data anywhere but within that territory.[22] Such restrictions raise the cost of doing business across borders and, in a digital ecosystem, the threat to efficiency is real. Further, they stifle the access of businesses and public sector bodies to cheaper and more innovative services, or force companies operating in multiple countries to contract excess data storage and processing capabilities.[23] For start-ups and small and medium enterprises (SMEs), this constitutes a serious obstacle to growth, to entering new markets, and to the development of new products and services.[24] The EU has adopted a regulatory framework for the free flow of non-personal data in the EU,[25] which lists some of the non-personal data as being data generated by artificial intelligence, the Internet of Things and machine learning as potential sources of non-personal data along with a few very specific examples.[26]

Overview of the paper

In view of the above, this paper will seek to address the following issues. Firstly, it will interrogate the way data (both personal and non-personal) has been dealt with by the EU as a yardstick, with the aim of imagining how a harmonized data regulation system that encompasses both personal and non-personal data would look either on a continental scale or on a regional scale within Africa. Emphasis will be placed on determining how legal instruments guide or mandate the identification of non-personal data. This is because, in addition to the already existing efforts to protect personal data, it is necessary to regulate how non-personal data is used to ensure that both personal and non-personal data can move freely across the continent and across the globe, underpinned by sound regulation and policies. Such free movement is necessary to reap the potential economic benefits and may aid in realizing Africa's development agenda and the Sustainable Development Goals (SDGs). With the central theme being that of free movement of data, the paper will then delve deeper into aspects such as the use of and liberalization of open data policies (the notion that specific data should be freely available for use and re-use, especially public sector information). The paper will then discuss, in addition to the potential legal conundrums that come with the liberalization of data and its movement, the cyber-security concerns that come with such a regulatory regime. This would be done by considering how the Malabo Convention protects personal data and Regional Economic Communities (RECs) and individual approaches by AU member states to cyber security.[27]

2. The European Union's approach to data

The European Union (EU) has been at the fore of establishing a comprehensive regulatory framework on data of both a personal and non-personal nature. Since 2014, the European Commission has developed a number of directives and laws to facilitate the development of a data-agile economy. Examples include the regulation on the free flow of non-personal data[28], the Open Data Directive[29], the GDPR[30] and the Cybersecurity Act.[31] The recently adopted EU Data Strategy[32] takes on an interdisciplinary approach to regulation of the data economy. The strategy is rooted in the need to expand the responsible use, demand and development of digital products and services within the European Single Market for the period 2020 to 2025 and is backed by the intention to make the EU a leader in a data-driven society. Therefore, by creating a single market for data, this will allow it to flow freely within the EU and across sectors for the benefit of businesses, researchers and public administrations.[33]

As has been stated before, the GDPR principally applies to the processing of personal data.[34] This extends to both an identified person and an identifiable natural person.[35] If this is applied practically, it therefore means that the GDPR and, by extension, data protection does not apply to anonymous information or information which does not relate to an identified or identifiable natural person. The same can be said for personal data which has been so diluted or encrypted that it is rendered anonymous because the data subject is no longer identifiable. It is on this background that the EU adopted the regulation on a framework for the free flow of non-personal data in the EU[36], also known as the FFD Regulation. The regulation makes it clear that it "applies to the processing of electronic data other than personal."[37]

The formulation of this regulation was rooted in the realization that the expanding Internet of Things (IoT), artificial intelligence and machine learning, which are major sources of non-personal data, continuously presented legal problems for legislators and the courts alike because there was no precedence on how to deal with such data. In a competitive environment where practices such as data analytics may establish a competitive advantage, non-personal data such as real-time traffic avoidance navigation has the potential to save corporations up to 730 million hours in transit time and up to €20 billion in labour costs among many other examples.[38]

Having realized the value and utility of non-personal data, the FFD regulation seeks to ensure four main objectives:

(i) The free movement of non-personal data across borders within the EU. In the same breath, it seeks to ensure that any interested organization that has the capacity and means to do so should be able to store and process data anywhere in the EU.

(ii) The availability of data for regulatory control. In this sense, it aims to ensure that public authorities retain access to data, even when it is located in another EU country or when it is stored or processed in the cloud.

(iii) The ability to effectively and easily switch between cloud service providers for professional users. The Commission has started facilitating self-regulation in this area, encouraging providers to develop codes of conduct regarding the conditions under which users can move data between cloud service providers and back into their own IT environments.

(iv) Full consistency and synergies with the cybersecurity package, and clarification that any security requirements that already apply to businesses storing and processing data will continue to do so when they store or process data across borders in the EU or in the cloud.

The GDPR already provides for the free movement of personal data within the EU[39] subject to compliance with/the provision of certain guarantees.[40] In this way, an amalgamation of all laws connected to data regulation in the EU ensures that there is a comprehensive and coherent approach to the free movement of all data in the EU.

Lessons from the EU approach

The key lessons to be taken from the European approach are that firstly, the EU has realized that various kinds of data exist, and it is not only personal data that is of value or worthy of protection/regulation. Secondly, that data is not valuable when it is stagnant. Rather, any value to be derived from data only emerges when data is allowed to flow/move freely across the EU. Thirdly, the EU's approach to data regulation takes the form of a multi-faceted approach. In addition to having adopted a data strategy that serves as a guide against which all legislative efforts must aspire to effectuate, there was the realization that to achieve the goals of the strategy, different legislation would have to be enacted, albeit with the same goal in mind. Because there are so many aspects to regulating data, and technology is constantly evolving, not only does the multi-faceted approach give more legal clarity and certainty on different regulatory issues, but it also makes it easier to amend and develop distinct parts of the law without disrupting ancillary legislative pieces. The effectiveness of this strategy, although still unfolding, has thus far yielded positive results and admiration from the rest of the world as evidenced by how many countries have 'borrowed' various provisions from the different EU laws for implementation within their domestic and regional regulatory efforts.

3. African regulatory approaches to the liberalization of data and its movement

The Free Movement of Data

The advent of the Internet presented the world with a means to send copious amounts of data to almost any part of the world with minimal cost. In fact, it can be said that the cost of sending data across borders costs no more than sending data within the same borders. The COVID-19 pandemic has highlighted just how important data flows are important for the global economy. Data flows have been shown to have influence in areas such as healthcare (contact tracing/medical research/vaccine production), business/ecommerce (online shopping, streaming services, virtual meetings/conferences) and socially (family video calls, online concerts). The extent to which these fields have been influenced (positively) is an indicator that in future, data flows will only continue to rise as more countries and sectors embrace digital transformation. It has already been determined that between 2007 and 2017, global data flows multiplied more than twenty-fold and it is expected that by 2022, the situation as of 2017 would have quadrupled (World Bank, 2021).

Within the African context, international and regional frameworks that facilitate cross-border data flows will be essential for the facilitation of a common market and by extension, the realization of the continental developmental goals, such as the realization of the African Continental Free Trade Area (AfCFTA)[41] and the African Union's Agenda 2063.[42] 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 localization clauses. Generally, data localization laws require that personal data about a nation's citizens or residents be collected, processed, and stored within the borders of the country (Bowman, 2017). Where a request is made that such data is transferred internationally, several approvals and a lot of bureaucracy must be observed.[43] Data localization 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 unauthorized activity such as profiling or surveillance by governments or any other third parties without consent (unless otherwise required under the law).[44] While it is understood that

it is essential for digital transactions to be supported by formidable regulatory frameworks in privacy, security, and consumer protection, such frameworks can impede the cross-border transfer and use of data by imposing substantial effort and costs on businesses, especially micro, small, and medium enterprises (MSMEs), thereby deterring international exchanges.[45]

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 organizations, individuals and countries.

Benefits of Cross-Data flows

Benefits for individuals

For individuals, the reach and influence of the Internet has already enabled their seamless interaction with people and organizations from across the world. In the same breath, individuals have also been exposed to goods and services from foreign markets that are available online and may be delivered in short periods of time where such products are physical.[46] As has been mentioned before,[47] the practice of data analytics has enabled organizations to cater for more geographic markets, giving those customers access to a wider range of goods and services based on their interests, wants and needs, which further improves competition in the markets and overall customer satisfaction.[48] Additionally, cross-data flows also enable individuals to carry out remote work from wherever they are in the world. The surge in remote work has come to be known as the "human cloud". The human cloud is defined as a budding set of online or digital marketplaces for labour where competent professionals and those looking to hire professionals can locate and engage one another in employment/work arrangements.[49] By the end of 2018, it was estimated that the money spent on using the human cloud spend was estimated to generate around US$ 82 billion globally, a figure that was expected to grow exponentially.[50] The facilitation of cross border flows will not only allow the host country the opportunity to export talent, but also the chance to reduce unemployment rates and generate foreign currency.

Benefits to the country

Free cross-border flows have enabled more national businesses and consumers to enter the digital commerce sphere, thereby encouraging the endorsement of data-driven business strategies and stimulating the national economy.[51] Public sector bodies and government departments also benefit from cross-border data flows allowing them to deliver better quality public services at a lower cost and pursue public policy objectives that might not otherwise be achievable.

Benefits to organizations

The free movement of personal data delivers social and economic benefits much faster than the alternative, which would require businesses to actively construct their back-offices and to streamline their processes and storage functions to serve multiple individual markets.[52] Countries that adopt regulatory regimes that support the free international transfer of data allow small, specialized organizations to establish an Internet presence that is simultaneously national and international.[53] In this way, it is possible to have services successfully adopted in one national market, then expanded to other markets, bringing rapid benefits for second and subsequent countries.[54]

A key advantage of the Internet is that it allows any organization, no matter how small, to use the Internet to market and deliver its ideas, goods and services, wherever data is allowed to flow. In this sense, if there are restrictions on the movement of data, organizations would not be able to provide information and products in response to individuals' requests.[55] Multinational organizations are also able to become more efficient by centralizing and virtualizing their internal operations. Examples of improved efficiency include the cost-effective expansion of business by utilizing flexible, cloud-based infrastructure, and specialist application service providers and minimizing investment in additional IT equipment.[56]

The COVID-19 pandemic's unseen benefit amid all the negatives is that more and more international businesses have seen the importance of adopting data-driven digital transformation strategies to secure their future. Such strategies tend to depend on being able to collect, analyze, process and store data across multi-country operations. The practice of data analytics becomes even more amplified as organizations seek to generate new customer insights and the performance of their operations and products.[57]

Data localization laws in Africa

This section gives an overview of some African states' data localization laws. In lieu of the views expressed in section 3 of this paper, that data localization laws do not support the free flow of data, the enactment and implementation of these laws, for example through hefty fines for using remote data storage, has detrimental effects. However, each state is entitled to enact and implement its domestic laws. The contribution of this paper is that in legislative and policy making processes, African states ought to consider the impact of data localization on data flows.

Cote-d'Ivoire

In 2013, The Ivory Coast/Cote-d'Ivoire enacted privacy laws,[58] which required firms to get pre-approval from the regulator before processing personal data outside of the Economic Community of West African States (ECOWAS).

Ghana

In 2019, Ghana enacted the Ghana Payment Systems Bill and Guidelines which, among other things, sets out the requirements to obtain a payment systems operator license, which pertains to local ownership and the appointment of Ghanaian directors. Prior to this, in July 2018, Ghana issued draft regulation that required all domestic transactions be processed by the Ghana Interbank Payment and Settlement Systems Limited (GhiPPS, which is wholly owned by the Central Bank of Ghana).

Kenya

Kenya's 2019 Data Protection Act[59] does not contain the explicit data localization provisions, which appeared in earlier drafts of the law. However, it still includes restrictive provisions governing personal data, which require explicit consent for transfers of "sensitive personal data"[60] and that data controllers ensure and provide proof that personal data transferred abroad receives the same protection as if stored within the borders of Kenya.[61] Regulations implementing these provisions are still being developed.

Proposed measures (2021)

Following the enactment of the 2019 Data Protection Act, Kenya has released three draft data protection regulations to aid in implementation of the Data Protection Act.[62] These are the Data Protection (General) Regulations,[63] the Data Protection (Registration of Data Controllers and Data Processors) Regulations[64] and the Data Protection (Compliance and Enforcement Regulations).[65] Under the proposed measures, the General Regulation requires that where data processing is done for the purpose of producing a public good, the processing should be carried out through a server and data centre located within Kenya's borders[66] and that at least one serving copy of the personal data should be stored in a data centre located in Kenya.[67] The regulations also include provisions on cross-border transfer of personal data. Under the General Regulations, it is required that before transferring personal data outside of Kenya, the recipient ought to know they are bound by legally enforceable obligations to ensure the same level of protection to the transferred personal data as that provided for under the Data Protection Act in Kenya and the General Regulations;[68] that the data subject is informed of the safeguards and the implications and risks involved in the cross-border transfer;[69] that the data subject has consented to the transfer of their data to that recipient;[70] that the transferring entity has taken reasonable steps to ensure that transferred personal data is not used for any unintended purposes;[71] and that the data subject's rights are safeguarded.[72] The General Regulations also provide that cross-border transfer of data may be allowed without restrictions where the transfer is "necessary" as provided under Section 48(c) of the Data Protection Act;[73]

where the requirements arbitrarily or unjustifiably discriminate against any person;[74] where the requirements impose a restriction on trade;[75] and where the restrictions on transfers of personal data are greater than are required to achieve the objectives of the Data Protection Act.[76] The General Regulations also prescribe the terms that are to be contained in cross-border transfer agreements between transferring entities and the recipients of personal data albeit without prescribing the template model standard clauses as is seen in the European Union.[77]

Nigeria

In 2015, Nigeria enacted broad data localization requirements as part of the Guidelines for the Nigerian Content Development in ICT.[78] In the guidelines, it is required that all telecommunication companies interested in hosting subscriber and consumer data within Nigeria should host such data within the country and in line with existing legislation.[79] The same applies to Networking Service Companies[80] and Data and Information Management Companies.[81]

In 2011, The Central Bank of Nigeria also introduced a local storage and processing requirement for entities engaging in point of sale (POS) card services.[82] Under guideline 4.4.8, all domestic transactions including but not limited to POS and ATM transactions in Nigeria must be switched using the services of a local switch and shall not under any circumstance be routed outside Nigeria for switching between Nigerian Issuers and Acquirers.[83]

Rwanda

In 2012, Rwanda enacted a regulation that all critical information data within government should be hosted in their national data centre.[84] In terms of indirect application of data localization laws, in 2017, Rwanda's telecommunications regulator fined MTN the sum of US$ 8.5 million for maintaining Rwandan customer data in Uganda and for running its IT services outside the country in breach of its license (CNBC Africa, 2017). Comments have already been made in the introductory section of *Data Localization Laws in Africa* in section 3 on the enactment and implementation of data localization laws. Further, it could be argued that the imposition of such large fines may chill investment by firms that wish to use remote data storage facilities.

Senegal

In 2021, and in the light of the new Government data centre being built in Senegal, President Macky Sall announced that all government data and applications will be hosted at the centre and that any data stored on foreign servers would be repatriated in hopes of strengthening Senegal's digital sovereignty (Swinhoe, 2021).

South Africa

In 2018, following the realization that domestic South African banks intended to move more of their transactions to global payment service networks, the South African Reserve Bank suspended the migration of all domestic transaction volumes from Bankserv (South Africa's bank-owned domestic payment switch) to international payment schemes.[85] The suspension was to remain in place until a new policy was developed and enacted. Such a policy has not yet been developed and enacted at the time of writing.

In 2013, South Africa enacted the Protection of Personal Information Act (the POPI Act),[86] but which only came into full force on the 1st of July 2021, makes the transfer of personal information outside of South Africa subject to certain exceptions. These include the requirement that the recipient of the data be able to offer complimentary protection of the data,[87] that the data subject consents to the data transfer,[88] that the transfer is necessary for the performance of a contract between the data subject and the responsible party[89] or for the conclusion/performance of a contract in the interest of the data subject[90] and if the transfer is for the benefit of the data subject.[91] While these are not explicit localization laws, there is concern as to how they will be interpreted and enforced, as they could become *de facto* data localization tools.[92]

Proposed measures

More recently, South Africa's "Draft National Policy on Data and Cloud" of 2021[93] recommends the adoption of data localization standards and local data processing for all data incidental to "critical information infrastructure"[94] and data mirroring for personal data.[95] It also states that all data generated in South Africa shall be the property of South Africa, regardless of the nationality of the firm involved in collecting it.[96]

Egypt

In Egypt, President Abdel Fattah el-Sisi ratified the Personal Data Protection Law[97] on the 13th of July 2020. The law aims to protect and regulate the collection and processing of personal data of Egypt's citizens and residents. In relation to data localization, the law prohibits the transfer or retention of personal data to a foreign country or territory without the permission of the Egyptian Data Protection Centre and unless that country or territory has adequate levels of personal data protection.[98] Egyptian Minister of Communications and Information Technology, Amr Talaat, was also quoted stating that the data protection law was formulated in support of the Ministry's efforts to localize the data centre industry and create a safe environment for the circulation of information within the cyberspace.[99] Egypt also belongs to the Arab Maghreb Union, who have so far not attempted to regulate data collectively as a union.

Angola

The Data Protection Law[100] draws inspiration from provisions found in the EU and Portuguese legal regimes for the protection of personal data. The enforcement authority, known as the Agência de Proteção de Dados (APD), was only created in October 2019 despite the law being created in 2011, and there is presently no significant level of enforcement. The law requires that the APD be notified prior to any international transfers of personal data to countries deemed to have an adequate level of protection[101] in addition to specific requirements that must be met such as consent of the data subject.[102] Angola also belongs to the Economic Community of Central African States (ECCAS), which in 2016 adopted a model law (with the support of ITU and EU). However, because ECCAS does not have binding community law instruments, only 3 member states out of 10 have adopted a national privacy law (Le Bihan, 2018).

Open data policies/standards

To compliment the call to enable liberalized cross border data flows, open standards/policies for data can also be particularly useful tools that make it easier for individuals and organizations to access, use, publish and share better quality data while simultaneously addressing cyber security concerns. Open standards for data are reusable agreements that necessitate the access, use, publication and the sharing of better-quality data (Open Data Institute, 2021). Open data standards can also be defined as sets of specifications or requirements for how specific sets of data should be made publicly available.[103]

They are particularly helpful because:

1. They increase interoperability: Data interoperability is a feature of datasets where data can be easily retrieved, processed, re-used, and re-packaged ("operated") by other systems with little to no effort.[104]

2. They improve comparability of data: Because open data standards enable easy access to datasets, they make it easier to compare data from different sources and to draw more concrete conclusions by drawing from a pool of like datasets.

3. They enable aggregation: By lowering the barriers to access to data, open standards for data encourage the publication of new data and better-quality data that is structured in a similar way, making it easier to combine them. In the process, the cost and complexity of combining similar data from multiple sources is significantly decreased (Open Data Institute, 2021).

4. They enable linkability: Open standards make it easy to combine diverse data sets to give useful insights.

Common uses of open standards for data

As has been stated, open standards are essential in aiding the creation of a strong data ecosystem. Within this ecosystem, there are data assets,[105] the organizations responsible for the operation and maintenance of the data assets, and guide that set out how to use, store and manage the data.[106] A strong data infrastructure is critical to fostering business innovation, driving better public services and creating healthy, sustainable communities.[107]

To promote common understanding

Many open standards exist today for different purposes and in different sectors. The commonality across all successful open standards is that they focus on tackling specific issues with reusable agreements that support better quality data. Therefore, where there is need for people and organizations to agree on common guidance, a shared language, or common models when solving problems, open standards are ideal.[108]

To support policy and legislation

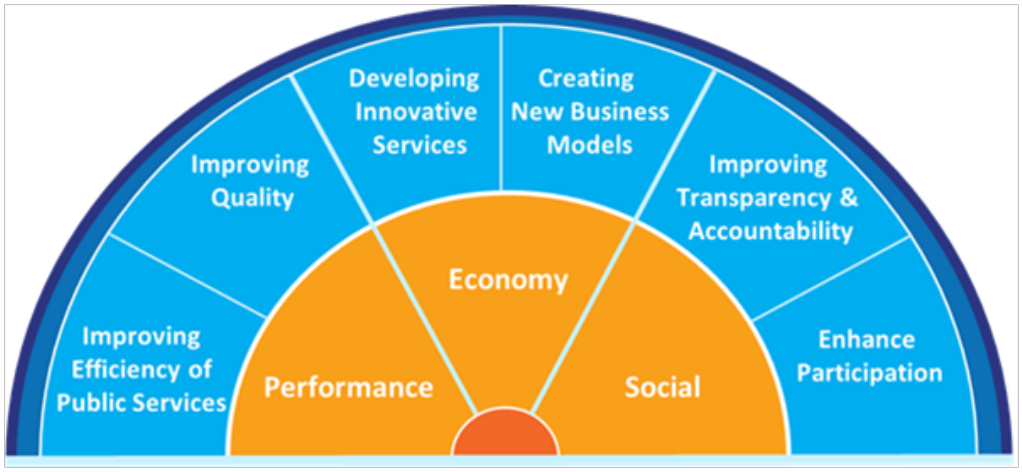
When implementing policies and substantiating legislation adopted or developed by governments and other public bodies, open standards for data can be useful support tools. By establishing standards on how to disclose data, how to automate compliance checks, how to aggregate or report on data, and in the process this can produce better quality data and strengthen data infrastructure.[109]

To fill gaps in a data infrastructure

A strong data infrastructure[110] is grounded on principles that promote accountability, transparency, business innovation, civil society and public services. Within the infrastructure are data assets, the organizations that operate and maintain them, and the regulations that describe how to use and manage the data.[111] It is therefore important that a strong data infrastructure is supported by open data standards. The identification of gaps is made easier by lessening the barriers to entry in data pools and the participation of more stakeholders.

Benefits of open data standards

The benefits of open data standards can be summarized using the image below.



Source: Image from data europa.eu[112]

Economic benefits

The economic benefits of Open Data Standards are of greater importance to this discussion. The crux of the benefits presented by open data standards are that standards create new commercial opportunities and ecosystems that encourage competition. First, standards help to deconcentrate authority. Well established market leaders and authorities are discouraged from using custom and proprietary formats and opt instead to make use of cooperatively produced and shared standards (Open Data Institute, 2021). This effectively levels the playing field for data production and data use, allowing new uses of data and new entries to the market.[113]

Therefore, by effectively reducing barriers to entry and the costs associated with the collection and aggregation of data in a particular sector, standards also allow more organizations to enter the ecosystem to provide more diverse products and services within the data ecosystem.[114] Examples include translation, conversion, combination, reporting, training, analytics, consumer products, business-to-business services, and more. Open standards for data mean that an organization can focus on providing value at any stage of the data pipeline.

Social benefits

Open data standards encourage multi-stakeholder collaboration. Essentially, developing a standard that is useful to the community and used by stakeholders needs multi-stakeholder collaboration. Multi-stakeholder collaboration connects people and organizations working within a sector. Data publishers are interested in

who else publishes data using standards, so that they can understand how issues were overcome and improve their processes. Data users are interested in connecting with other data users with similar goals or issues. In the process, a focus for shared vision may be developed (Open Data Institute, 2021). When people and organizations with a common problem or an unmet need work together to reach an agreement about producing or using better-quality data, the people and organizations involved need a shared vision of the open standard, including a common understanding of the problem they are trying to solve and agreement on how they will solve it.[115]

In the process, an open standard for data can aid in coordinating activities to understand the problem or unmet need; agreeing on the current ecosystem, data assets, concepts and language in use; agreeing on the data and models needed to solve the problem or meet the need; pooling resources to work towards clearly defined goals for the standard, leading to mutually reinforcing activities; forming connections across sectors to support the standard's goals, which can help to build trust, peer learning and peer support; and producing and reusing tools that strengthen data infrastructure, including supporting data publishers, providing data users with insight, and making it easier for developers to create tools and services.[116]

Policy impacts

From a policy perspective, open standards can support implementation of policy. In the past, policy makers requiring organizations to publish data have focused on what data must be published but not on how. This leads to situations where disclosure is widespread, but the data is difficult to collate and use. By adopting open standards for data and linking them to policy and regulation, policy makers can make data more usable, provide clear guidance on how to disclose data, automate compliance checks, data aggregation and reporting open standards for data provide clarity to data publishers, the opportunity for stakeholder engagement and help ensure consistent and comparable results (Open Data Institute, 2021).

Technological benefits

The key technological benefits of open data are that standards produce better quality data.[117] Open standards encourage the development of tools and services to help data publishers produce good quality data, including tools to validate, preview and compare data (Open Data Institute, 2021).

Open standards can advise data publishers how often data should be published. Some standards include ways to share publication schedules, publication dates, location and methods of accessing data. Sharing this information makes it easier to trust published data.[118]

In addition, when data is published consistently, the time, cost and processes involved in using it are reduced. Consistent publication encourages the creation of new tools and services that are designed to take advantage of data that conforms to a standard.[119]

Example of open data standards in use

Probably the most famous open data standard is the General Transit Feed Specification (GTFS), which is a standard developed by tech giant google. The GTFS allows public transit agencies to publish their transit data in a format that can be interpreted and used by a variety of software applications (GFTS, 2021). Because of the interoperability of open data standards, GTFS data can be used by many other third-party software applications for a variety of purposes. Examples include trip planning, timetable creation, mobile data, data visualization, accessibility, analysis tools for planning, and real-time information systems (GFTS, 2021). Among public transportation data formats, GTFS stands out because it was conceived to meet specific, practical needs in communicating service information to passengers. It is designed to be relatively simple to create and read for both people and machines.[120] The value of an efficient transport system has real implications on the economy of a country, but because it is so easy to access and share data in this manner, efficiency is amplified even beyond borders.

Cyber-security concerns

The movement of data entails considerable security risks, hence the need for cybersecurity and the protection of both personal and non-personal data. As indicated above, the Malabo Convention is the only current continental legal instrument that focuses on the protection of personal data and cyber security. It is relevant to data governance to the extent that it pertains to these two aspects, which are integral to data governance. Indeed, as noted above, the AUC is shepherding the development and formulation of the Africa Data Policy Framework, which is informed, in part, by the Malabo Convention. 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 organizations"(Yang et al., 2019). Leading up to the adoption of the Malabo Convention in 2014, several RECs adopted regulatory instruments on privacy and cybersecurity (Ncube, 2016). These are: ECOWAS' Supplementary Act on Personal Data Protection within ECOWAS (2010); the ECOWAS Directive on Fighting Cybercrime (2011); the Common Market for Eastern and Southern Africa (COMESA) Model Cybercrime Bill (2011); the Southern African Development Community (SADC)'s Model Law on Data Protection and a Model Law on Computer Crime and Cybercrime (2012). Of these, only the SADC Model covers both privacy and security; however, as it a non-binding instrument, and consequently the Malabo Convention stands out as the only binding instrument regulating both privacy and security. Further, according to its preamble, it "embodies the existing commitments of AU member states at sub-regional, regional and international levels to build the information society," making it the continental blueprint. Accordingly, this section reprises the Malabo Convention's provisions on cybersecurity and privacy. A**s already noted above, this section is succinct, due to the coverage of the same content, in greater detail, by another paper which constitutes part of the project.**

Privacy

As indicated above, the Malabo Convention focuses on the protection of personal data (privacy) rather than non-personal data. Its definition provision sets out the following fundamental definitions:

> **Personal data** means any information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity
>
> **Personal data file** means all structured package of data accessible in accordance with set criteria, regardless of whether or not such data are centralized, decentralized or distributed functionally or geographically
>
> **Sensitive data** means all personal data relating to religious, philosophical, political and trade-union opinions and activities, as well as to sex life or race, health, social measures, legal proceedings and penal or administrative sanctions

It then turns to the regulation of the processing of personal data which is defined as:

> any operation or set of operations which is performed upon personal data, whether or not by automatic means such as the collection, recording, organization, storage, adaptation, alteration, retrieval, backup, copy, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination and locking, encryption, erasure or destruction of personal data

The core of such regulation consists of the basic principles governing the processing of personal data as set out in Article 13. These are:

Principle 1: Principle of consent and legitimacy of personal data processing

Principle 2: Principle of lawfulness and fairness of personal data processing

Principle 3: Principle of purpose, relevance and storage of processed personal data

Principle 4: Principle of accuracy of personal data

Principle 5: Principle of transparency of personal data processing

Principle 6: Principle of confidentiality and security of personal data processing

Their meaning is the same as that of the GDPR's principles as set out at section 2 above. They are supplemented by Article 14, which sets out specific principles for the processing of sensitive data. Another core component of privacy in the Malabo Convention is its Section IV on the Data Subjects' following rights: Right to information (Article 16); Right of access (Article 17); Right to object (Article 18) and Right of rectification or erasure (Article 19). Personal Data Controllers have the following obligations: Confidentiality obligations (Article 20); Security obligations (Article 21); Storage obligations (Article 22) and Sustainability obligations (Article 23).

Cybersecurity

The Malabo Convention does not contain a definition of cybersecurity, which would have been useful to underpin a significant aspect that it regulates. Yang et al (2019) define cybersecurity as "the practice of protecting computer and network infrastructures, the operating systems, software programmes run on the infrastructures, and all the data stored or transmitted through the infrastructures from digital attacks and any other misuse" (Yang et al., 2019). Chapter three of the Convention is intended to promote cybersecurity and prevent cybercrime. Article 24 addresses national cyber security frameworks, specifically national policies and strategies relating to the Critical Information Infrastructure (CII). The Malabo Convention defines CII as "the cyber infrastructure that is essential to vital services for public safety, economic stability, national security, international stability and for the sustainability and restoration of critical cyberspace."

Article 25 then proceeds to address legal measures, namely: (1) cybercrime national legislation; (2) regulatory authorities; (3) citizens' rights; and (4) protection of critical infrastructure. According to Article 25.1 national cybercrime legislation is required to effectively sanction "criminal offences acts which affect the confidentiality, integrity, availability and survival of information and communication technology systems, the data they process and the underlying network infrastructure". Data is expressly mentioned here, so some national cybersecurity measures in relation to data is mandated. Further, Article 25.2 requires "effective procedural measures to pursue and prosecute offenders." Article 26 then proceeds to require state parties to establish a national cyber security system comprising of the necessary institutions, which are appropriately staffed, to oversee implementation of the legal measures through actions, including responding to cyber security incidents, and coordination and cooperation in forensic investigations and prosecution, amongst others. Such legal measures and their implementation must have due regard to the human rights of citizens.[121] State parties are also required to establish legislative or regulatory measures to protect priority sectors that are important for national security by, for instance, introducing more severe sanctions for offences in these sectors.[122]

Article 26 provides for some further detail regarding the national cybersecurity system through mandating each state "to promote the culture of cyber security" and suggests measures that may include cyber-security plans and awareness campaigns.

Article 27 proceeds to deal with national cyber security monitoring structures, which state parties are required to adopt for cyber security governance within a national framework. Article 28 provides for international cooperation through harmonization, encouraging states to offer each other mutual legal assistance and the exchange of information, along with the use of existing means for international cooperation. Article 29 then provides for offences that are specific to ICTs. It requires state parties to create offences relating to attacks on computer systems, for instance to gain unauthorized access and data breaches such as the interception or attempted interception of computerized data. There are also provisions relating to content-related offences in Article 29 and the adaptation of property offences and sanctions to ICTs in articles 30-31, but these are not pertinent to the chapter's area of focus.

The provisions of the Malabo Convention have a baseline, but more is needed for a robust approach to privacy and security for non-personal data because its privacy provisions are primarily for personal data and its cybersecurity provisions place emphasis on national infrastructure or the CII.

In summary, this section shows that most African states need to create, enhance or strengthen their privacy and cybersecurity frameworks. In view of the aims of both the AfCFTA and the Digital Transformation Strategy to facilitate and grow e-commerce and digital trade in Africa, it will be important to align domestic frameworks. This gives a measure of certainty for entrepreneurs trading in multiple jurisdictions. As also indicated above, and reinforced below, the negotiations of the AfCFTA e-commerce protocol will provide a platform to agree on fundamental data governance principles.

4. Conclusion

This paper exposes in part that one of two things are happening on the continent. 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 by mostly individuals. It will therefore be imperative that a trusted data environment 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 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.[123] This will go a long way in moderating the concerns related to the free movement of data. Also, because most African states are still in a developmental state, with some more advanced than others, capacity building in relation to data protection, cybersecurity and institutional data governance in relevant agencies should be prioritized and realized through policy and asset allocation. In addition, where institutional arrangements and regulations come about because of the consultations and dialogue, these arrangements ought to be established through inclusive, consultative and transparent processes. Accountability and transparency are answer to most of the concerns that follow the shift to data liberalization and use.

As argued at section 2 above, it is important to highlight that personal and non-personal data should not be treated the same, hence distinct approaches exist in other parts of the world. While the concerns around the protection and regulation of

personal data are legitimate, non-personal data which has a lot of value within itself should not be subject to the same scrutiny. In this regard, lessons can be drawn from the approach that the EU has taken in ensuring that the two are distinct (see key lessons outlined at section 2.1 above).

The current position, as summarized at section 3 above, confirms that most African countries' attempts at regulating data have overly pre-occupied themselves with personal data, neglecting non-personal data. In the same breath, because personal data is of higher value, it is no surprise that protection laws in this regard may be overbearing. While the current forms of data localization laws may be thought of as being national governments' attempts to assert sovereignty over data, a borderless medium, the reality is that as more countries enact updated data protection frameworks, it is highly likely that some policy makers will propose more stringent data localization laws as they believe that the best way to protect data is to store it within a country's borders. However, evidence has shown that the security of data does not depend on where it is stored. Instead, by allowing for the free movement of data across international borders, cyber security concerns are less likely to materialize. By allowing cloud service providers to draw from data flows from all over, they will be able to establish best practices in cyber security. Similarly, while cloud computing does not guarantee security, it will lead to better security because implementing a robust security programme requires resources and expertise, which many organizations and African countries lack. But large-scale cloud computing providers are better positioned to offer this protection. In fact, the security of data depends primarily on the logical and physical controls used to protect it, such as strong encryption on devices and perimeter security for data centres. The nationality of who owns or controls servers or which country these devices are located in has little to do with how secure they are. 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. Furthermore, because a comprehensive data regime also makes provision for data sovereignty, data specificity should also be prioritized. Data specificity is used to refers to countries being able to specify what kinds of data can and cannot move freely. Data specificity should be prioritized to avoid unintended restrictions on productive data sharing.

As the AfCFTA and the Digital Transformation Strategy for Africa (2020-2030) seek to increase e-commerce and digital trade in Africa, it is important to consider how supporting the free movement of data across Africa can enhance these efforts. It has been shown that cross-border data flows are instrumental and have the potential to greatly influence a new economic resurgence for the continent, as can be drawn from experiences of countries or regional bodies that have adopted a liberal approach to data regulation. Their experience has evidenced that data localization does not serve the purpose that many think that it does and in actual fact could be thought of as being counterproductive in terms of securing and drawing value from data. Most African countries that have enacted data localization laws in one way or the other have done so under the justification that the security of data is dependent on where it is stored or

collected, which is in fact a fallacy. It has been shown that open policies towards cross border data flows have generated better security measures and better revenues for the countries that have adopted these systems. The African continent can learn from these experiences now to adequately support the free flow of data. It is also necessary to emphasize that the adoption of open standards for data, which will complement the cross-border data flows, ensuring that they are the flows are conducted in a safe and transparent manner and to ensure that barriers into accessing the data economy are reduced, thereby encouraging more players to get involved within the data economy. By adopting open data standards and decentralizing the power to collect, use and aggregate data, participation in the data economy is encouraged and the chances of illegitimate uses of data are lessened. In the process, governments are also afforded the opportunity to work on and strengthen their impact in key areas such as policy, technology and development and the economy. Such an approach recognizes the importance of cybersecurity and supports it within an ecosystem that encourages open data participation.

Ultimately, there is need to adopt a cohesive legal approach that is unambiguous and offers protection and obligations across the continent, while taking cognizance of the value that the liberalization 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.

Notes

1. This work is based on research supported in part by the National Research Foundation (NRF) of South Africa (Grant number: 115716). Any opinion, finding and conclusion or recommendation expressed in this material is that of the authors and the NRF does not accept any liability in this regard.

2. OECD Glossary of statistical terms "data" available at https://stats.oecd.org/glossary/detail.asp?ID=532 accessed on 28/04/2021.

3. Ibid.

4. Math is fun what is data available at https://www.mathsisfun.com/data/data.html accessed on 28/04/2021.

5. Diffen 'Data vs Information 'available at https://www.diffen.com/difference/Data_vs_Information accessed on 28/04/2021.

6. Ibid.

7. Ibid at 2.

8. Art 4(1) of the GDPR

9. 'Personal Data' (General Data Protection Regulation (GDPR) <https://gdpr-info.eu/issues/personal-data/> accessed 17 January 2022.

10. ibid.

11. Explained: What is Non-Personal Data?' (The Indian Express, 27 July 2020) <https://indianexpress.com/article/explained/non-personal-data-explained-6506613/> accessed 17 January 2022.

12. Privacy International 2020 is a crucial year to fight for data protection in Africa 3rd March 2020 available at https://privacyinternational.org/long-read/3390/2020-crucial-year-fight-data-protection-africa accessed on 30/04/2021.

13. The General Data Protection Regulation 2016/679.

14. Ibid.

15. Research ICT Africa (RIA) Online consultation: Call for submissions on Africa Data Policy Framework 17 Jul 2021 https://researchictafrica.net/2021/07/17/online-consultation-call-for-submissions-africa-data-policy-framework/

16. African Union Digital Transformation Strategy for Africa 2020 – 2030 available at https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030

17. African Union, 2020. Decision on the African Continental Free Trade Area (AfCFTA). Assembly/AU/Dec.751(XXXIII). https://www.tralac.org/documents/resources/cfta/3176-au-assembly-decision-on-the-afcfta-february-2020/file.html

18. WTO 'Negotiations on e-commerce advance, eyeing a statement at MC12' https://www.wto.org/english/news_e/news21_e/ecom_10nov21_e.htm

19. Patrick Breyer v Bundesrepublik Deutschland Case C-582/12.

20. Bird and Bird 'EU data economy: Data-related legal, ethical and social issues' available at https://www.twobirds.com/~/media/pdfs/eu-data-economy-legal-ethical--social-issues.pdf Accessed on 30/04/2021.

21. Ibid.

22. Ibid.

23. Ibid.

24. Ibid.

25. Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303.

26. Bird and Bird supra note 20.

27. Since another paper in this project considers the Malabo Convention, national and REC data protection regulatory instruments in detail, this paper gives those aspects brief and succinct treatment to minimize overlap and duplication.

28. Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the EU.

29. Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information.

30. The General Data Protection Regulation Supra note 13.

31. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

32. https://op.europa.eu/en/publication-detail/-/publication/ac9cd214-53c6-11ea-aece-01aa75ed71a1/language-en

33. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en

34. Article 2.1. GDPR Supra note 13.

35. "[that is] one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (Article 4.1 of the GDPR) including quasi-identifiers and metadata (Article4.1).

36. The FFD Regulation supra note 28.

37. Article 2.1. of the FFD Regulation supra note 28..

38. https://medium.datadriveninvestor.com/digital-europe-200-billion-investment-strategies-for-artificial-intelligence-data-and-blockchain-f7f656e66603.

39. Article 1(3) of the GDPR states that the overarching goal of the GDPR is to ensure that "the free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons regarding the processing of personal data."

40. See Chapter 2 (Art 5 to 11) of the GDPR.

41. https://openknowledge.worldbank.org/bitstream/handle/10986/34139/9781464815591.pdf

42. https://au.int/sites/default/files/documents/33126-doc-01_background_note.pdf

43. Ibid.

44. Data protection and privacy laws | Identification for Development https://id4d.worldbank.org/guide/data-protection-and-privacy-laws.

45. World Bank "Creating value in the data economy.

46. GSMA ”Cross-Border Data Flows: Realizing benefits and removing barriers“ available at https://www.gsma.com/publicpolicy/resources/cross-border-data-flows-realising-benefits-and-removing-barriers

47. See note 9, Russom, Philip. "Managing big data." (2013) TDWI Best Practices Report, TDWI Research at 5.

48. GSMA “cross border data flows

49. Analysts, Staffing Industry. "The human cloud, the gig economy & the transformation of work." (2017). Available at https://www2.staffingindustry.com/content/download/246507/9128496/HumanCloudSummary2017_170912.pdf

50. Ibid.

51. GSMA “Cross border data flows

52. Ibid.

53. Ibid.

54. Ibid.

55. Ibid.

56. Ibid.

57. Ibid.

58. LAW No. 2013 450 dated June 19, 2013 on the protection of personal data available at https://ictpolicyafrica.org/fr/document/4wo0y6uby6j

59. The Data Protection Act No 24 of 2019.

60. Section 44 of the Act read with Section 25.

61. Section 25(h) of the Act.

62. Supra note 59.

63. Data Protection (General) Regulations, 2021 available at https://www.odpc.go.ke/resources/data-protection-general-regulations-2021/

64. Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021 available at https://www.odpc.go.ke/resources/data-protection-compliance-and-enforcement-regulations-2021/

65. Data Protection (Compliance and Enforcement Regulations), 2021 available at https://www.odpc.go.ke/resources/data-protection-registration-of-data-controllers-and-data-processors-regulations-2021/

66. Regulation 25(1)(a) of the Data Protection General Regulations.

67. Regulation 25(1)(b) of the Data Protection General Regulations.

68. Regulation 38(1)(a) of the Data Protection General Regulations.

69 Regulation 38(2) of the Data Protection General Regulations.

70. Regulation 38(1)(b) of the Data Protection General regulations.

71. Regulation 38(1)(c) of the Data Protection General regulations.

72. Section 38(1)(d) of the Data Protection General regulations.

73. Regulation 40(1)(a) of the of the Data Protection General regulations.

74. Regulation 40(1)(b) of the Data Protection General regulations.

75. Regulation 40(1)(c) of the Data Protection General regulations.

76. Regulation 40(1)(d) of the Data Protection General regulations.

77. Regulation 39 of the Data Protection General regulations

78. Guidelines for Nigerian Content Development in Information and Communications Technology (ICT) of 2015 and as amended in Aug 2019. Available at https://nitda.gov.ng/wp-content/uploads/2020/11/GNCFinale2211.pdf

79. Section 11.1.3 of the Guidelines for the Nigerian Content Development in ICT.

80. Section 12.1.4 of the Guidelines for the Nigerian Content Development in ICT.

81. Section 13.1.2 and 13.2.3 of the Guidelines for the Nigerian Content Development in ICT.

82. The Central Bank of Nigeria's mandatory 2011 Guidelines on Point of Sale (POS) Card Acceptance Services available at https://www.cbn.gov.ng/cashless/POS_GUIDELINES_August2011_FINAL_FINAL%20(2).pdf

83. Guideline 4.4.8 of The Central Bank of Nigeria's mandatory 2011 Guidelines on Point of Sale (POS) Card Acceptance Services

84. Article 17 of the Ministerial order N°001/MINICT/2012 available at https://www.rlrc.gov.rw/fileadmin/user_upload/LawsofRwanda/Laws%20of%20Rwanda/7._Administrative/5.9.%20State%20Finance/5.9.3.%20Procurement/5.9.3.3._M._Instructions_Procurement_of_ICT_goods_and_services_by_public_institutions.pdf

85. Cory N, Dascoli L " How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them" Information Technology and Innovation Foundation Available at https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost

86. The Protection of Personal Information Act No 4 of 2013 available at https://popia.co.za/

87. Section 72(1)(a) of the POPI Act.

88. Section 72(1)(b) of the POPI Act.

89. Section 72(1)(c) of the POPI Act.

90. Section 72(1)(d) of the POPI Act.

91. Section 72(1)(e) of the POPI Act.

92. Cory N, Dascoli L Supra Note 85.

93. The Draft National Policy on Data and Cloud available at https://www.gov.za/sites/default/files/gcis_document/202104/44389gon206.pdf

94. "National critical information infrastructure" as defined in section 9 of the Policy means all ICT systems, data systems, databases, networks (including people, buildings, facilities and processes), that are fundamental to the effective operation of the Republic of South Africa.

95. Policy Intervention 10.4.1.

96. Policy Intervention 10.4.4. of the Draft National Policy on Data and Cloud.

97. The Personal Data Protection Law (Law No. 151 of 2020)

98. Article 14 of the Data Protection Law of 2020

99. 'Egypt New Data Law Supports Data Center Localization' (/ Daily News..., 5 August 2020) <https://www.datacenterplanet.com/data-center/egypt-new-data-law-supports-data-center-localization/> accessed 11 November 2021.

100. The Data Protection Law (Law 22/11)

101. Section VI of the Data Protection law

102. Article 34 of the Data Protection Law

103. Open Data Standards Directory open data standards definition available at https://datastandards.directory/ accessed 28/08/2021

104. https://aims.gitbook.io/open-data-mooc/unit-4-sharing-open-data/lesson-4.2-introduction-to-data-interoperability

105. The term data asset is used to refer to data that is expected to generate future revenues. This differs from one industry to the other and ultimately what is considered a data asset depends on the relevant business model. Examples include design and methodology, knowledge/know-how, user input, sensor data, calculated data etc. See 7 examples of a data asset available at https://simplicable.com/new/data-asset

106. "When to use open standards for data" Open Data Institute, 2021.

107. Ibid.

108. Ibid.

109. Ibid.

110. Data infrastructure consists of data assets supported by people, processes and technology.

111. When to use open standards for data" Open Data Institute, 2021.

112. The economic benefits of open data. Available at https://data.europa.eu/en/highlights/economic-benefits-open-data accessed 09/10/2021.

113. Ibid.

114. Ibid

115. Ibid.

116. Ibid.

117. In her book 'Executing Data Quality Projects', Danette McGilvray defines data quality as "the degree to which data can be trusted for any required use".

118. Ibid.

119. Ibid.

120. Ibid.

121. Article 25.3.

122. Article 25.4.

123. Chapter 7 of the GDPR

References

Bowman, C. 2017. “Data localization laws: An emerging global trend”. *Jurist*, 6 January 2017. Available at https://www.jurist.org/commentary/2017/01/courtney-bowman-data-localization/.

Ncube, Caroline B. 2016. “Recent developments in African regulation of cybercrime: An overview of proposed changes to the South African framework”. *Journal of Internet Law*, 19(7): 3–20.

Chaytor, Batrice. 2020. AfCFTA: An enabler of digital trade and e-commerce. Available at https://resilient.digital-africa.co/en/blog/tech_voices/afcfta-an-enabler-of-digital-trade-and-e-commerce-1-4/.

CNBC Africa. 2017. “Rwanda utilities regulatory authority fines MTN US$ 8,5M‘ 17 May 2017. Available at https://www.cnbcafrica.com/2017/rwanda-utilities-regulatory-authority-fines-mtn-us-85m-non-compliance/.

GTFS. 2021. Making public transit data universally accessible. Available at https://gtfs.org/ accessed 10/10/2021 GTFS (2021): Making Public Transit Data Universally Accessible available at https://gtfs.org/ accessed 10/10/2021.

Jean-Francois Le Bihan. 2018. Regional regulatory capacity building. GSMA Africa Policy Day 16 July 2018. Available at https://www.gsma.com/publicpolicy/wp-content/uploads/2018/07/M360-Africa-Policy-Day-Presentation.pdf accessed on 11/11/2021.

Jeremy, Daniel. 2021. Data protection laws in Africa: What you need to know. CIO Africa 15 February 2021. Available at https://www.cio.com/article/3607734/data-protection-laws-in-africa-what-you-need-to-know.html?upd=1619734077195 accessed on 29/04/2021.

Manzo, Valentina. 2019. The internet of things and intellectual property rights: The protection of data 2019 WIPO Academy, University of Turin and ITC-ILO - Master of Laws in IP - Research Papers Collection - 2017–2018 Available at SSRN: https://ssrn.com/abstract=3387417 at 1.

Okonjo-Iweala, Ngozi. 2021. Remarks at the Centre for the Study of the Economies of Africa (CSEA)’s webinar on data governance in Africa: Pathways for strengthening confidence in the digital economy, 11 August 2021 https://www.youtube.com/watch?v=Vnvh2JZx8PA.

Open Data Institute. 2021. What are open standards for data? Available at https://standards.theodi.org/introduction/what-are-open-standards-for-data/ Accessed 28/08/2021.

Russom, Philip. 2013. Managing big data. TDWI best practices report, TDWI Research at 5.

Swinhoe, D. 2021. Senegal to migrate all government data and applications to new government data center. Data center dynamics, June 23 2021. Available at https://www.datacenterdynamics.com/en/news/senegal-to-migrate-all-government-data-and-applications-to-new-government-data-center/.

World Bank. 2021. Creating value in the data economy: The role of competition, trade, and tax policy. World Development Report 2021: Data for better lives. March 24, 2021 available at https://www.worldbank.org/en/publication/wdr2021.

Yang, L., Li, J., Nko, N., Prickett, T.,Chao, F. 2019. "Towards big data governance in cybersecurity". *Data-Enabled Discovery*, Appl. 3, 10 (2019). https://doi.org/10.1007/s41688-019-0034-9 at 1.

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