

STRENGTHENING DATA GOVERNANCE IN AFRICA

Project Inception Report



Contents

ACKNOWLEDGEMENT	2
EXECUTIVE SUMMARY	3
BACKGROUND AND OBJECTIVE OF THE STUDY	3
2 PRELIMINARY FINDINGS	6
3 AFRICAN CONTINENTAL FREE TRADE AREA (AFCFTA)	17
4 MOVING FORWARD	19
References	20
APPENDICES	22
1 Overview of data governance legislation in Africa by country*	22
2 Summary of Stakeholder Consultations	23



ACKNOWLEDGEMENT

Lead Authors: Sone Osakwe (Research Fellow at CSEA) and Adedeji Adeniran (Director of Research at CSEA).

Contributors: We thank the following CSEA staff who provided technical support and assistance at various stages of the study: Mustapha Saeed, Ezra Ihezue, Michael Ajifowo and Adebola Adedoyin. We also appreciate Thelma Obiakor's input and suggestions.

In addition, the authors will like to thank The William and Flora Hewlett Foundation for providing the grant that made this study possible. Finally, we wish to extend special gratitude to the stakeholders who participated in our consultation sessions, and whose insights contributed invaluable to this report.

EXECUTIVE SUMMARY

This inception report focuses on the emerging trends in Africa's digital and data environment. The study builds a case for mobilizing action at both regional and national levels, to strengthen data governance frameworks in Africa, particularly in view of the ongoing regional economic integration initiatives under the African Continental Free Trade Area (AfCFTA). We advocate for stronger data policies in Africa as a development tool for bridging identified gaps that could put the region at a disadvantage, and as a means of building greater confidence which is a requirement for growing the digital economy. The findings suggests that while the potential of digital technologies is yet to be fully exploited in Africa, the region has witnessed a surge in the use of digital platforms and tools in recent years. This has influenced the ease and manner in which data gathering and exchange occurs, resulting in heightening concerns around potential data abuse. In response, national efforts and domestic legal frameworks on data governance are gradually increasing in Africa, although rather slowly as there are still significant policy gaps. While the magnitude of the data policy gaps vary across different member countries, African countries have so far largely been unable to match the pace of change in the new data driven global economy. There is also a lack of uniformity in policy approaches being adopted by member states.

An equally disturbing observation is the inadequacy of implementation strategies in place; there is a general deficit in institutional capacity to support a well-functioning data governance environment in Africa. Therefore, further investigation to gain a deeper understanding of the major challenges and constraints to effective data governance is necessary, in order to draw up appropriate intervention strategies. A common regional approach to data governance is also likely to yield faster results by building upon lessons from previous regional efforts and leveraging the enforcement and structural advantages of the AfCFTA.

1 BACKGROUND AND OBJECTIVE OF THE STUDY

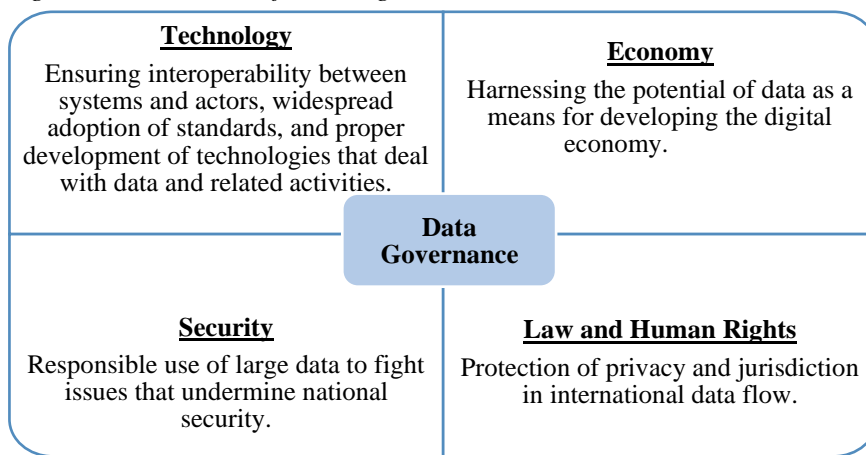
The emergence of digital technologies and increased usage of internet-based platforms is rapidly changing the way individuals, businesses and governments around the world operate. This has contributed to advancements in not just how data and information is collected, analyzed, used and distributed, but in the importance attributed to data as a valuable resource. Technologies that leverage data have the potential to instigate radical improvement in key areas of economic and social life such as the healthcare systems, financial services, education, governance and public safety. Greater access to data can potentially shrink the information gap in business operations, and between the state and its citizens. The ability to generate and analyze data in the fastest and most sophisticated form is therefore the driving force of the evolving digital economy (UNCTAD, 2019)¹. While this trend creates development opportunities especially for emerging economies, it poses risks and challenges in preserving the integrity of information systems and data resources (African Union Development Agency - NEPAD, 2020) as anyone with an internet connection or digital device has the ability to gather and share information across borders. Thus, if not properly managed or mitigated, data abuse could impede progress in maximizing data resources for public good and socio economic development.

According to the International Finance Corporation (IFC), Africa's digital economy is gradually expanding and expected to grow even faster by about 57% in the next five years. Sustaining such level of digital economic growth as an enabler for regional integration requires increased connectivity and data sharing among African member states. To ensure that local African businesses can compete favourably on the global stage, data access and interoperability is essential since cross-border trade in goods and services are increasingly reliant on cross-border flow of information related to demand, supply, logistics and regulatory processes. Closer economic ties such as the newly implemented AfCFTA tend to encourage unhindered data flow across jurisdictions. However, the cross-border dimension of data flow and susceptible nature of data to unauthorized access, privacy violations, misuse and abuse, theft, manipulation, unfair practices and exploitation presents concerns for policymakers and regulators. Some additional areas of concern relate to determining data ownership, consent management, and curbing cybercrime (Macmillan, 2020). These concerns have been further heightened during the COVID-19 era with increasing reports of data abuse.

With the increased amount of data currently being collected and the growing need for states to safeguard national sovereignty and individuals' human rights over their data, countries around the world are grappling with developing data governance rules on how data production and flow is governed locally and when interacting with the rest of the world. This includes a framework of policies, laws, regulations and processes that enable, guide, and make market participants accountable for how data is collected and used to generate insights, stored, shared and protected, and establishing regulators to enforce these laws (Sacks & Sherman, 2019). Trust in the data ecosystem is therefore central to the concept of data governance. An effective data governance policy should typically address the inherent risks in data sharing while ensuring that a wide variety of data can be accessed and used to achieve its greatest economic and social potential. This will enable innovation and responsible use of data/evidence by governments and businesses to improve outcomes for people. Gonçalves (2020) summarizes the key features of a good data governance framework as presented in figure 1 below:

¹ For the purpose of this report, we refer loosely to economic activities that are dependent and enabled by information, communications and digital technologies.

Figure 1: Focus areas for data governance



Considering that the world’s leading digital platforms are concentrated in a few countries - United States and China, Africa is currently at the receiving end (being primarily a platform user) of the fallout of the choices and activities of these digital platforms providers. In view of the data revolution and increasing threats, more African countries have started recognizing the importance of data governance. However, studies suggest that the existing mechanisms for data regulation in Africa is generally inadequate in addressing data threats (Belle, et al., 2018; Ademuyiwa & Adeniran, 2020; Ilori, 2020). The pace at which African member states are able to introduce and revise data policies and strategies is much slower than the constantly evolving global digital and data trends. It is important to note though that digital maturity and the level of data policy adoption and implementation varies across different member states. Given that most African countries are inundated with a wide range of development challenges relating to insecurity, hunger and poverty, the issue of digitalization and data governance had hitherto been relegated to low priority in the broader development agenda. There is thus a digital divide among Africa countries; the level of internet penetration and data infrastructure is uneven. These existing weaknesses and disparities represent an enormous obstacle to the successful uptake of the regional development goals under the AfCFTA, as consistent digital transformation strategies and data governance rules across the continent is a prerequisite for an enabling environment that engenders trusts and confidence in data systems, and supports greater cross-border digital trade and integration.

There is therefore a need to find a balance between encouraging free data flow and information sharing among African member states and doing so in line with fundamental data governance principles. For this goal to be achieved, it is necessary to understand the peculiar issues stalling advanced data governance practices in African countries. Therefore, this project inception report seeks to detail our initial findings from a problem scoping exercise that assessed the following:

- ✓ Trend in digital growth and data threats on the continent
- ✓ Present landscape for governing data use and sharing in Africa
- ✓ Role and scope for a harmonized regional data governance structure under the AfCFTA to increase the chances of better outcomes for an integrated and inclusive digital economy in Africa.
- ✓ Areas for further investigations to gain deeper insights to the factors hindering advancement of data governance on the continent.

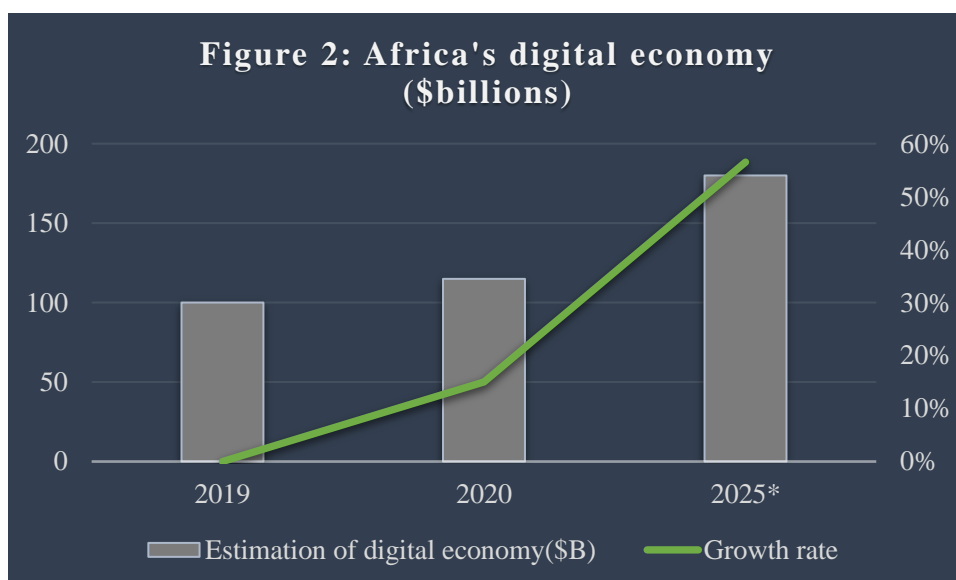
To answer the above questions, we zero in on the growing number of studies on the state of digitalization and data governance on the continent. We then consult with subject experts and practitioners to share practical experiences on data regulation issues. The main objective of the report is to increase awareness and contribute to debate on the importance of data governance as a catalyst for long-term social framework for trust in the digital economy, and the need to deepen/strengthen national efforts with a regional approach to data governance.

2.1 CURRENT DIGITAL AND DATA TRENDS IN AFRICA

Although Africa’s contribution to the global digital economy and ICT advancement is still largely insignificant when compared to other digitally developed regions, recent trends show a steady expansion of the region’s digital economy, and an uptake in the volume of digital transactions in various sectors ranging from online market places, financial technology services, mobile and internet subscriptions. While there is still a lot of road to cover in digital development, the growth being recorded in the region is promising. We highlight some of these growth trends below:

2.1.1 Value of Africa’s digital economy forecasted to grow much faster

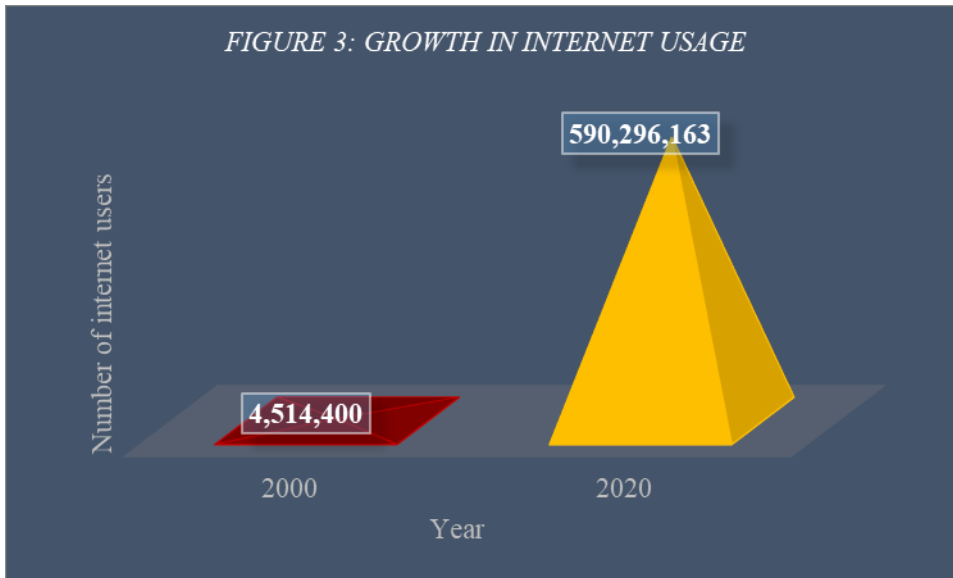
The contribution of economic activities in digital trade and other internet enabled business operations increased from \$100billion to \$115billion between 2019 and 2020, and has the potential to reach \$180 billion by 2025, accounting for 5.2% of the continent’s gross domestic product (GDP).



Source: [Author’s Elaboration of International Finance Corporation](#)

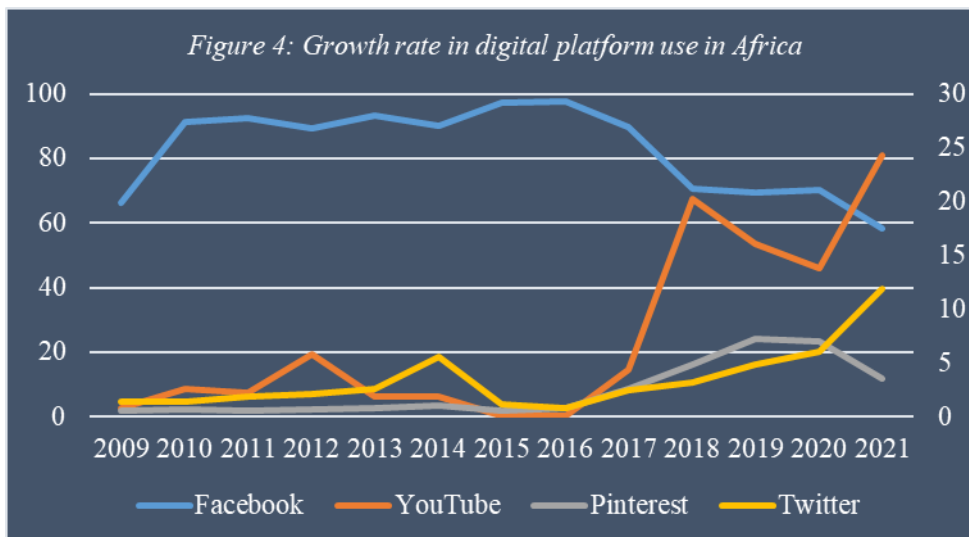
2.1.2 Rise in platform usage and subscribers

Internet penetration in Africa remains low but has improved over time, with a growing number of citizens able to access and use the internet. Figure 3 shows that the number of internet users has grown from less than 5 million Africans in the year 2000, to almost 600 million people as of last year, representing a little lower than half of the total population.



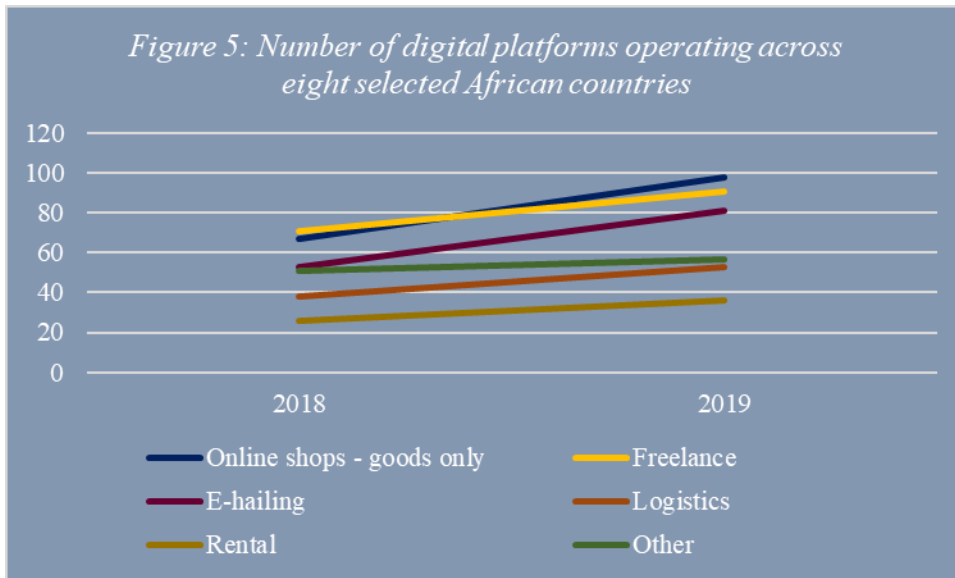
Source: [Author's Elaboration of Internetworldstats](#)

Similarly, even though user preferences for popular international digital platforms keep changing, the overall effect is a consistent increase in total number of users of these platforms in Africa as depicted in Figure 4.



Source: [Author's Elaboration of Statcounter](#)

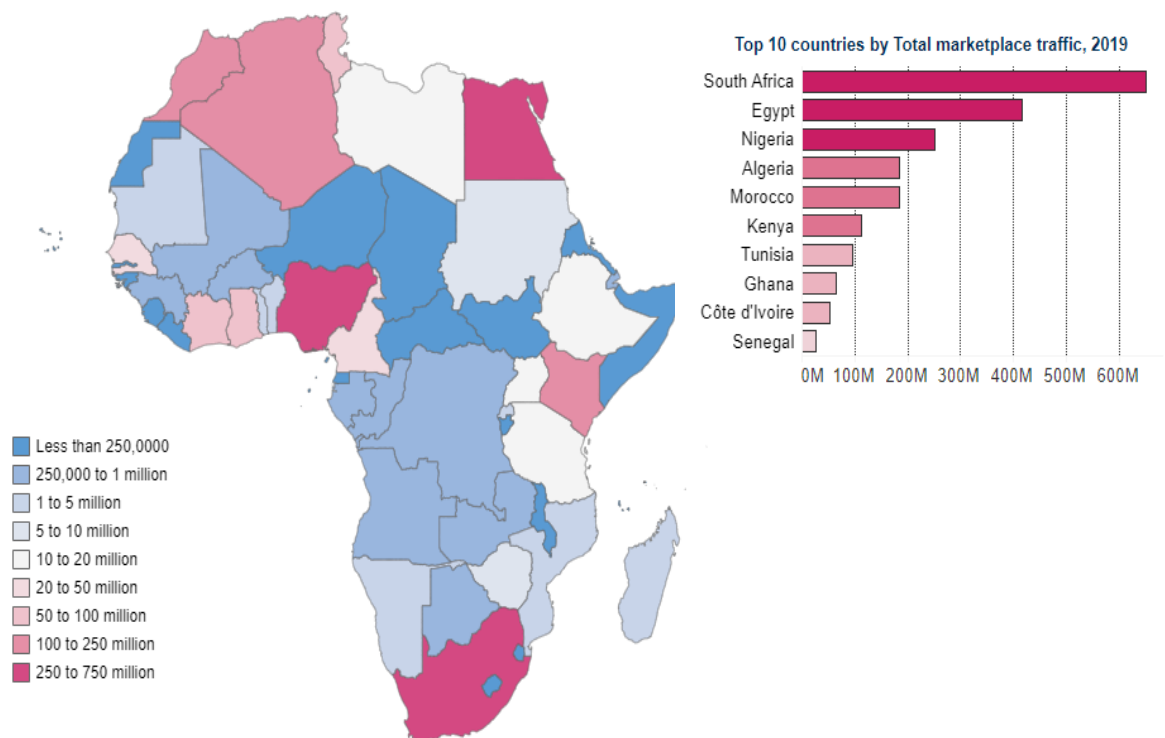
In terms of number of homegrown online platforms operating in multiple member states, data from Insight2Impact shows the numbers are increasing. In 2019 alone, the numbers rose by over a third from the previous year in the countries surveyed (Figure 5). The study further highlights that while approximately four out of every five digital platform operating in Africa is local, average number of users per platform is three times greater for foreign platforms originating outside the region's borders, than local platforms. This can be attributed to the advantage that foreign platforms; entering the market earlier and amassing a larger market share ahead of fledgling local platforms.



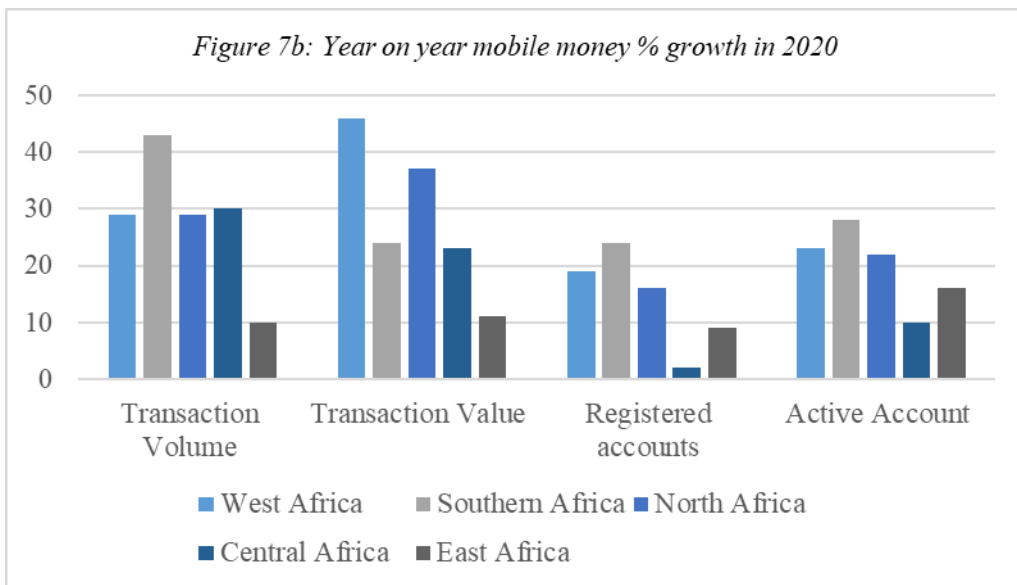
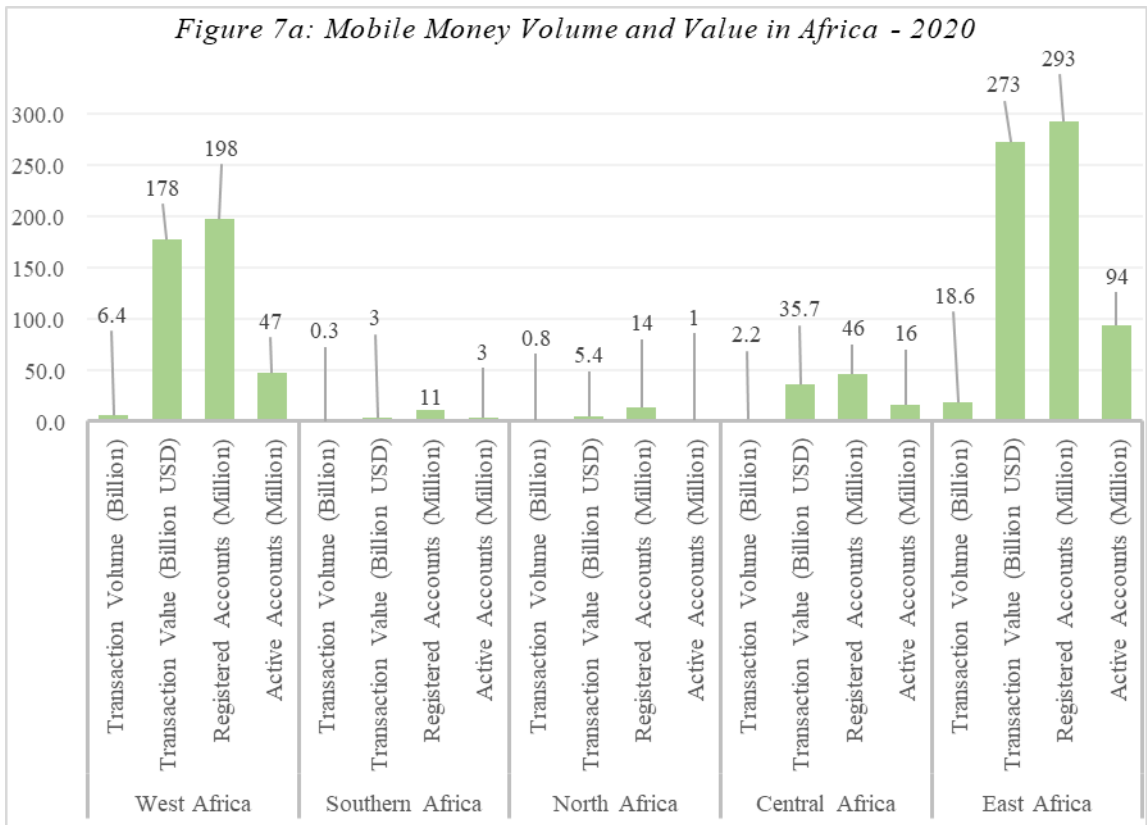
Source: [Author's Elaboration of Insight2Impact](#)

E-commerce and digital finance are among the most dynamic sectors of the digital economy. For instance, the number of visitors to online marketplaces for buying and selling of physical goods in Africa is on the rise. In 2019 alone, there were over 2 billion total visits to these marketplaces, with South Africa, Egypt and Nigeria recording the highest traffic (refer to Figure 6). Ernst and Young's 2019 report on the Fintech industry indicates that Africa's Fintech landscape has grown at an annual rate of approximately 24% over the last ten years, particularly payment gateways. A significant contributing factor is the expansion of mobile subscriptions which has enabled growth in convenient mobile money products. Figure 7a and 7b gives a snapshot of Africa's mobile money growth - the fastest growing in the world.

Figure 6: Total online marketplace traffic in Africa



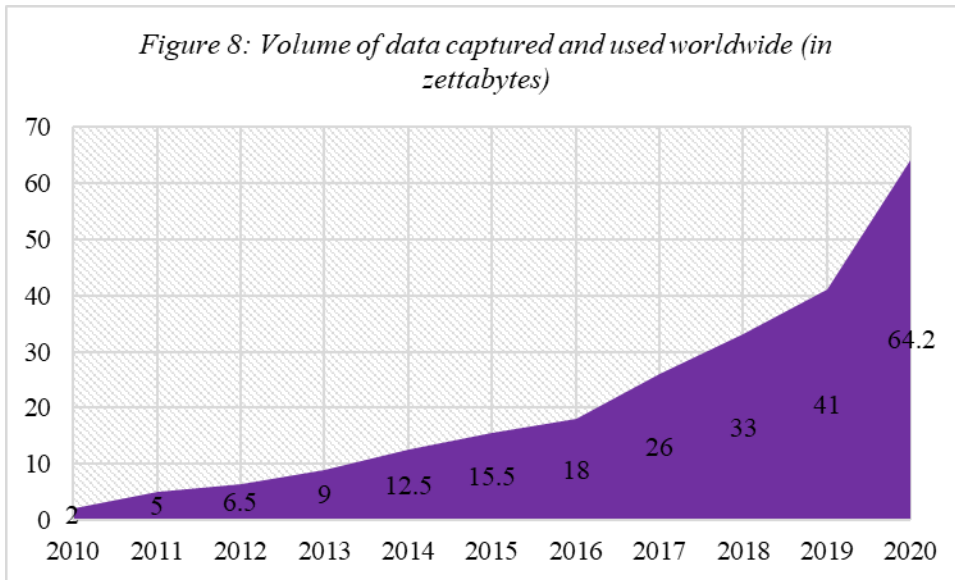
Source: [International Trade Center - African Marketplace Explorer](#)



Source: [Author's Elaboration of GSMA - Mobile Money Report](#)

2.1.3 Increase in volume and complexity of data

Proliferation of digital platform usage translates to increased ease and volume of information gathering. Although the total volume of information and data collected through digital devices and consumed within the continent is not readily available, a look at the global statistics provides some insight. On the average, the volume of data generated in the past ten years worldwide has grown by 45% annually, and expected to grow even faster in coming years. Figure 8 shows the growth trajectory so far:



Source: [Statista](#)

2.1.4 Increase in data threats

In view of the above digital and data spike, reported cases of data threats and associated revenue losses are now on the rise. Incidence reports vary. A few examples include: online tax and benefits fraud, cyber-attacks causing public service disruption, data leaks from servers of government parastatals, credit card theft such as automated teller machine skimming resulting in unauthorized duplication of credit card details, social engineering tricks to persuade unassuming victims into divulging personal information, and mobile sim card intercept attacks. Figure 9 illustrates the economic impact of such data threats and attacks.

Figure 9a: Estimated direct/indirect losses from cybercrime in Africa (\$billions)

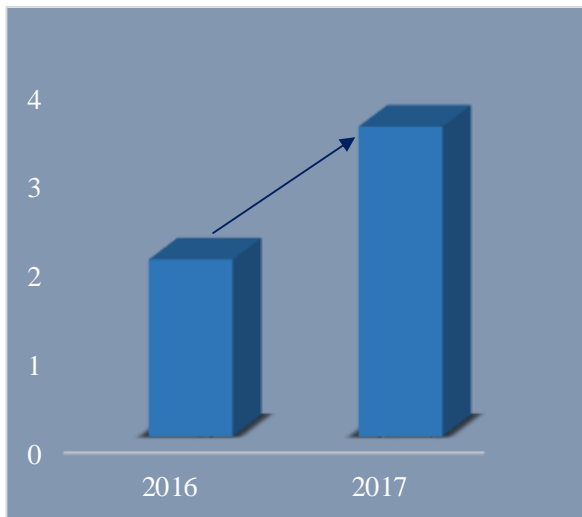
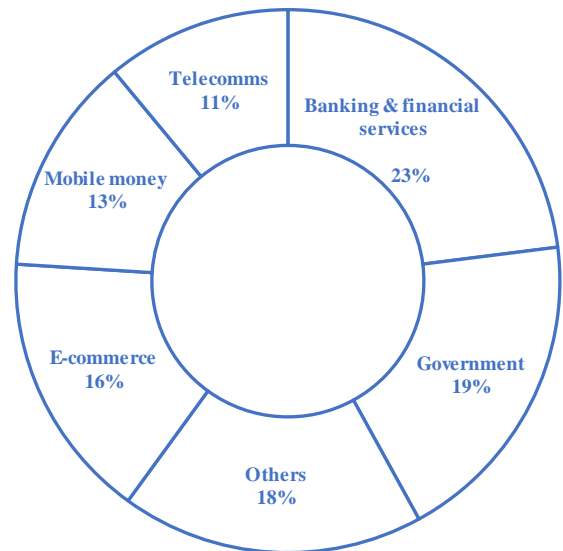


Figure 9b: Share of losses per sector

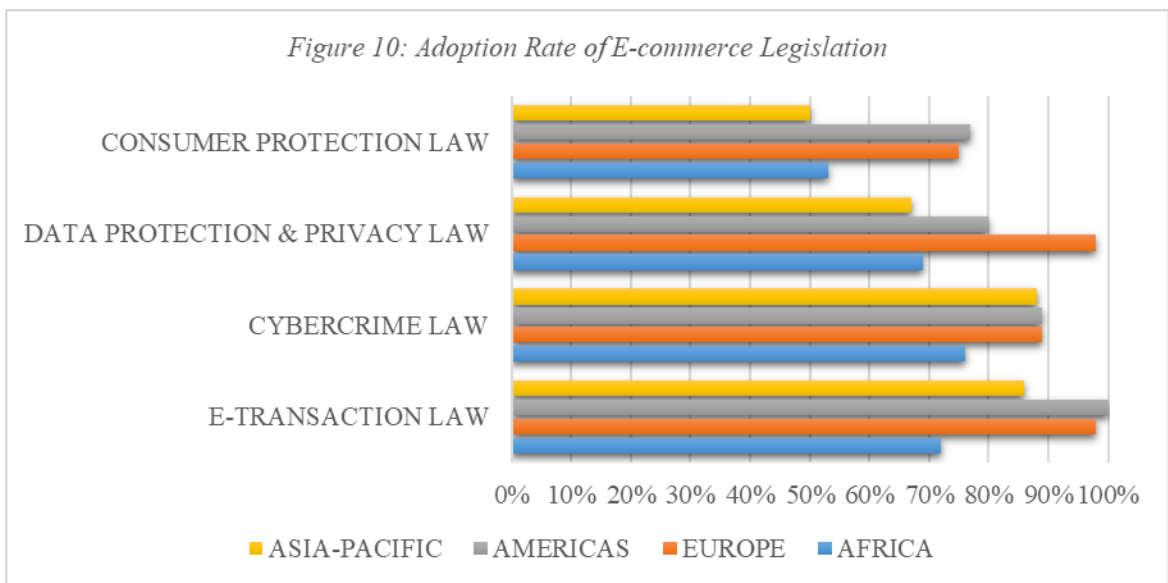


Source: [Author's elaboration of Serianu's Africa Report](#)

2.2 STATE OF DATA GOVERNANCE IN AFRICA: COUNTRY LEVEL

2.2.1 Slow enactment of data regulations/rules and enforcement

Our initial findings show that data governance in Africa is developing howbeit slowly. The degree of enactment, adoption and enforcement of data governance regulations varies across African countries. These variations are mostly attributable to differences in individual institutional capacities of respective governments to legislate and implement appropriate policies. Over a third of the total number of African countries still do not have any form of legislation on data and privacy protection, making Africa the continent with the least data governance prevalence (Ademuyiwa & Adeniran, 2020). The United Nations Conference on Trade and Development (UNCTAD) global progress tracker on the adoption rate of legislation to engender trust in the digital economy as summarized in Figure 10 further buttresses the gap in existing data governance rules in Africa when compared to other regions like Europe (Appendix 1 shows more details by country).



Source: [Author's Elaboration of UNCTAD's E-Commerce Legislation Index](#)

It is important to note that UNCTAD's index only focuses on the existence of relevant legislation, and not adequacy, effectiveness, or scope of coverage of such laws. A closer look at the countries where legislation is in place reveals that implementation remains a challenge. Also, most of these legislation are limited in scope, not extensive and do not address local context. For instance, out of twenty African countries assessed in a study conducted by Ademuyiwa & Adeniran (2020), besides Kenya, Benin and Mauritius, other data regulations did not cover the right to portability and accountability measures such as documentation requirements. Another example is the case of Nigeria, despite accounting for the greater portion of Africa's internet and mobile-cellular users and e-commerce traffic, the country does not yet have dedicated legislation in force to guide and regulate e-commerce transactions².

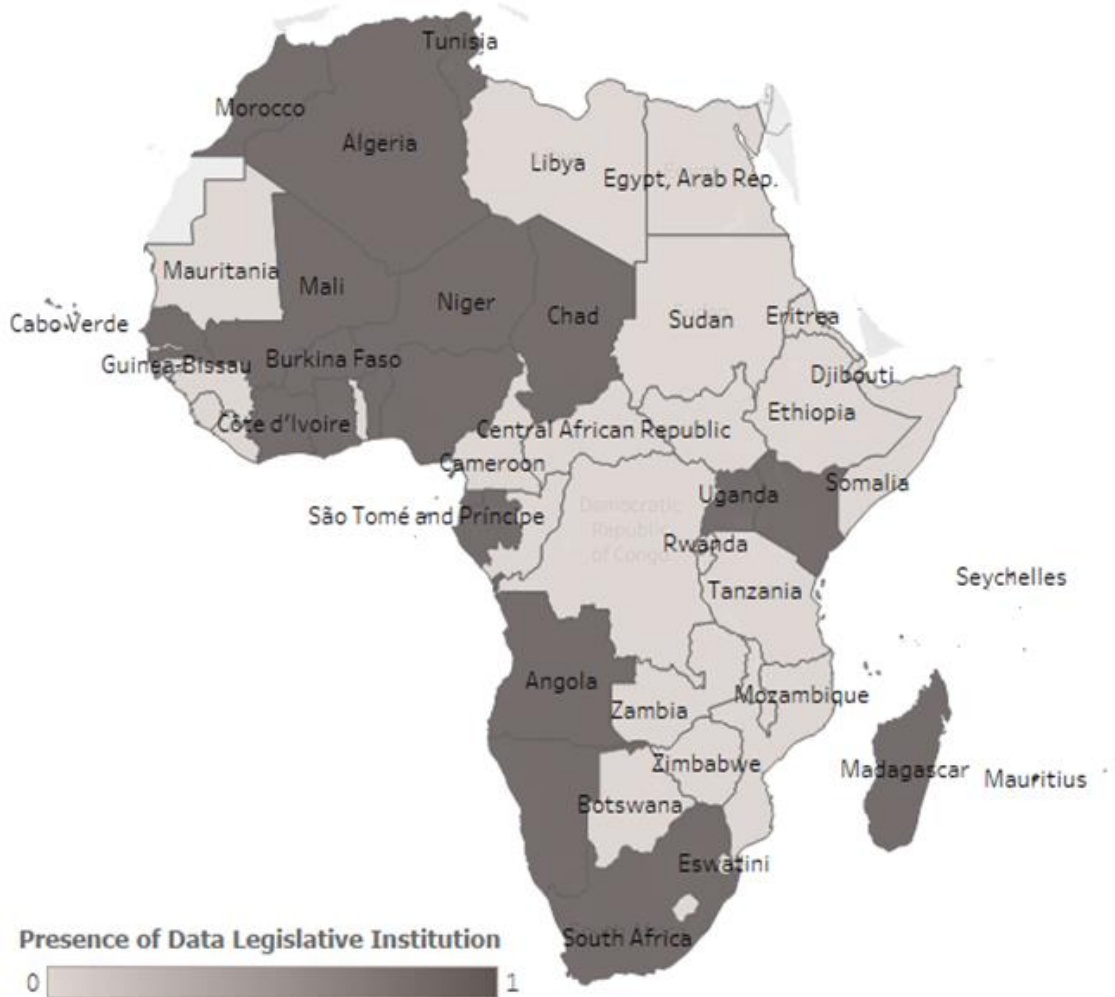
Our consultations with stakeholders revealed an equally important challenge of poor implementation of data laws in addressing the data governance gap in member states³. Thus, even where digital

² [Web traffic or proportion of internet users as share of population by country](#)

³ Details on stakeholders consultation are contained in Appendix 2.

regulations exist, enforcement is weak due to lack of institutional capacity and dearth of digital infrastructure at national level. Most African countries lack competent regulatory agencies with the requisite autonomy, skills and resources needed to draft, support or implement effective data regulations. Figure 11 shows that less than half of African nations have data regulatory agencies.

Figure 11: African countries with a designated regulator or agency for data governance issues



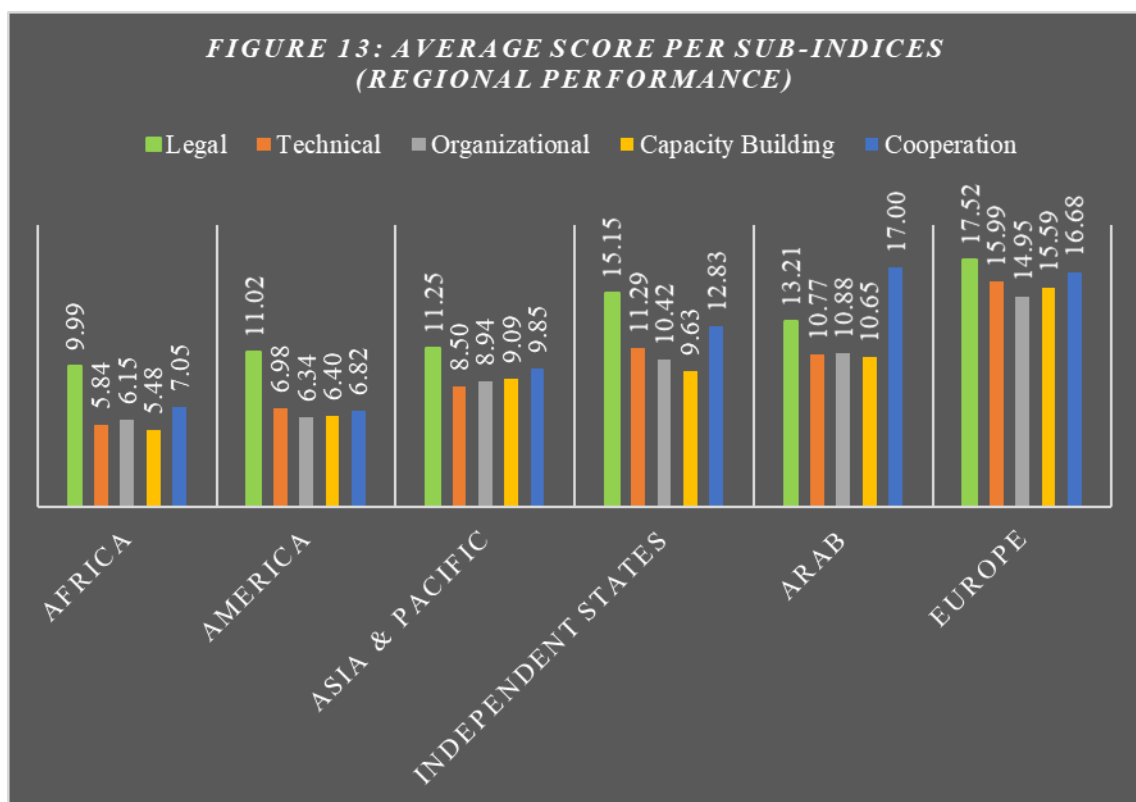
Source: [World Legal Information Institute](#)

low commitment towards promoting cybersecurity

A review of the International Telecommunication Union’s global cybersecurity index that measures the level of 193 countries’ commitment to promoting cybersecurity, reveals that only a fifth of African countries have a high level of commitment and meet standard requirements for curbing cybercrime. Most African countries showed either low or medium commitment levels in the aspect of cyber laws / standards and other areas such as: public awareness campaigns, having a national emergency response team to address incidence reports, capacity building for regulators, technical resources, and collaboration with similar agencies in other jurisdictions. Figures 12 and 13 provide a snapshot of Africa’s performance on the index.

Figure 12: Country commitment to cyber security

Commitment	Count	Countries
High	11	Mauritius, Egypt, Tanzania, Ghana, Tunisia, Nigeria, Morocco, Kenya, Benin, Rwanda and South Africa.
Medium	11	Uganda, Zambia, Côte d'Ivoire, Botswana, Cameroon, Chad, Burkina Faso, Malawi, Zimbabwe, Senegal and Sudan.
Low	32	Algeria, Togo, Gambia, Libya, Ethiopia, Sierra Leone, Mozambique, Madagascar, Guinea, Mauritania, Eswatini, Cabo Verde, Somalia, Sao Tome and Principe, Congo Republic, Seychelles, Angola, Namibia, Gabon, Niger, Mali, Guinea-Bissau, Liberia, Lesotho, South Sudan, Democratic Republic of Congo, Comoros, Central African Republic, Burundi, Djibouti, Eritrea and Equatorial Guinea.



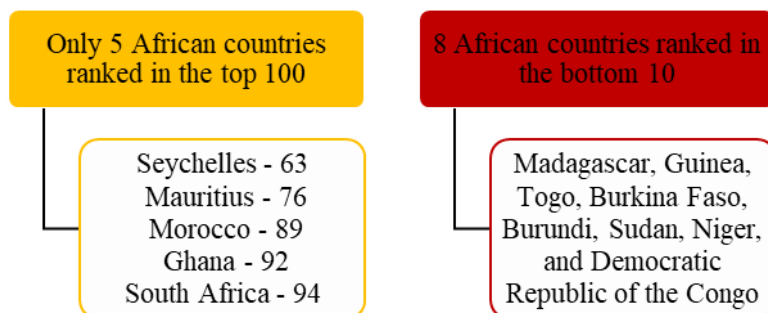
Source: [Author's Elaboration of ITU Global Cybersecurity Index](#)

2.2.2 Restrictions in information integration and data flow

Information flow between African countries is rather low. The DHL Global Competitiveness Index for 2020 measures how capital, trade, people and information flow freely across the world⁴. For the information flow sub-index, only five African countries are ranked in the top hundred of countries surveyed. The low score is reflective of the limited data flow and interconnectedness among African countries and with the rest of the World.

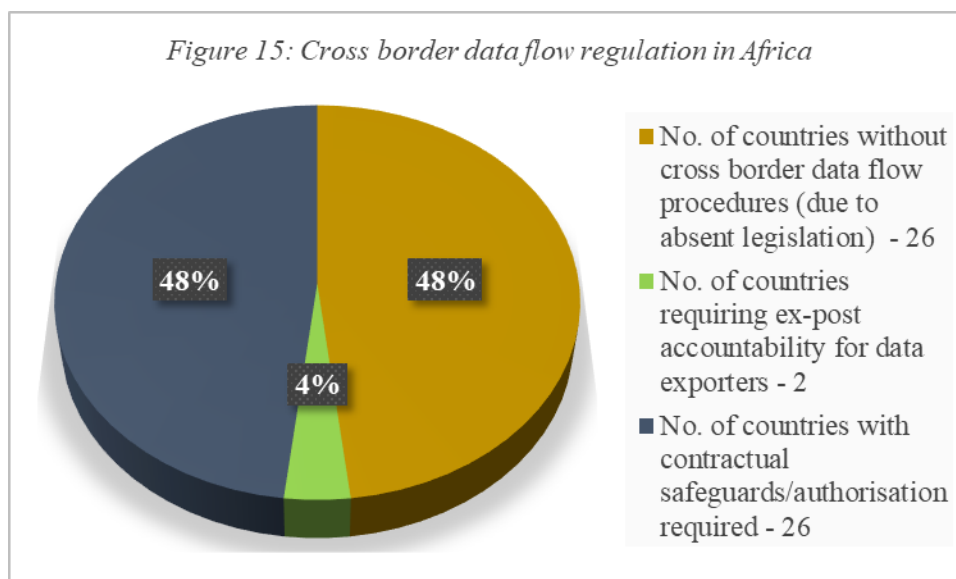
⁴ [DHL Global Competitiveness Index - 2020](#)

Figure 14: Information connectedness



Source: [Author's Elaboration of Global Connectedness Index](#)

The findings from Smart Africa's study on cross border data flows on the continent are similar and highlight significant restrictions on intra-African data mobility as shown in Figure 15. This may be a result of a lack of reciprocal data protection laws and processes among African nations. The lack of data sharing among member states could make regional trading difficult and cumbersome.



Source: [Author's Elaboration of Smart Africa's Study on Africa's Cross Border Data Flows](#)

Bearing in mind the above limitations at country level, a comprehensive harmonized regional framework that ensures effective governance and use of digital data could help strengthen national efforts.

2.3 STATE OF DATA GOVERNANCE IN AFRICA: REGIONAL LEVEL INITIATIVES

A regional data governance framework comprises a set of coordinated and consistent policies, legal guidelines and mechanisms that are well defined and clear, establishing specific rules and responsibilities on the appropriate treatment of data as it flows into, within, and out of a region or continent. Such framework is usually designed with the overarching goal of breaking down barriers to data mobility across member states, in order to build an interconnected/common data system for collective benefit. There are some existing regional initiatives to foster better data governance in Africa; however, the momentum so far has been weak resulting in minimal success. Examples of some of these initiatives are presented below:

- ✓ African Union Convention on Cyber Security and Personal Data Protection⁵: also known as the Malabo Convention was signed as far back as 2014, detailing basic principles and guidelines on safeguarding data. Signatories to the convention are obligated to establish domestic policy measures that conform to the guidelines set out in the convention, to curtail and mitigate occurrences of cybercrime and privacy violations. As at the time of this report, the benchmark of fifteen (15) countries required to ratify the convention has not been met.
- ✓ African Union Digital Transformation Strategy (2020-2030)⁶: The strategy is not a convention and therefore not binding; rather it presents policy objectives and recommendations on promoting growth in intra-African e-commerce and digital trade. It comprises strategies for strengthening a single digital market in Africa in line with the goals of the AfCFTA. The objective is to eventually use it as an operational tool and roadmap to guide member countries.
- ✓ Declaration on Internet Governance and Development of Africa's Digital Economy 2018⁷: This is an undertaking by heads of state of member governments of the African Union, acknowledging the importance of the digital economy, and committing to take necessary legal and regulatory actions to ensure that Africa's digital economy thrives.
- ✓ Personal Data Protection Guidelines for Africa⁸: A joint initiative of the Internet Society and the African Union. It is a set of guidelines with an emphasis on the importance of engendering trust in online transactions, as a means to a sustainable and productive digital economy. It also offers guidance on how individuals can take a more active role in protecting their data while recognizing that more often than not, the eventual outcome is dependent on positive actions by other stakeholders.

Regional Economic Communities (RECs) within Africa have also taken some steps to improve data governance, although some of these set rules are recommendations and not mandatory requirements. Examples include; Economic Community of West African State has a supplementary act dated 2010 on personal data protection that requires the establishment of a legal framework for data protection and privacy at the national level, and the establishment of national data protection agencies. Seven of the fifteen member states have enacted legislation in compliance with the agreement. The East African Community has a framework for cyber laws adopted in 2010 which recommends that each member state develop a regulatory regime for data protection but makes no specific recommendations on the selection of the law. Southern African Development Community SADC Model Law on Data Protection (2013) is another example. This law serves as a model for member countries to ensure data accountability.

Despite the highlighted regional efforts to strengthen data governance, the overall data legislative framework in Africa remains fragmented and not harmonized.

⁵ [AU Convention on Cyber Security and Personal Data Protection](#)

⁶ [AU's digital Transformation Strategy \(2020-2030\)](#)

⁷ [Declaration on Internet Governance](#)

⁸ [Personal data protection guidelines for Africa](#)

2.4 BENEFITS OF A REGIONAL DATA GOVERNANCE APPROACH

A structured regional data governance agenda can enable Africa maximize gains from digital trade, complement countries' capabilities, support a healthy flow of information that fosters fair competition and positions member states for the influx of digital investments. We highlight specific benefits to be drawn:

- ✓ Facilitate trust, data openness and more consistent policymaking: An environment of trust will ensure more transparency, openness and invariably better data use for policymaking. Having a set of uniform standards and guidelines across the region that meets global expectations and fits domestic/national realities, would help create some level of consistency and confidence, since each member country would be bound to comply with minimum standards for ensuring ethical use and protection of data. Such framework can provide some form of checks and balances and support greater compliance monitoring. Greater confidence in similar data protection measures and avenues for redress will allay digital users' fears and encourage increased e-commerce transactions. It can also reduce the proliferation of data localization laws and engender a more conducive environment for the free flow of data on the continent. It would deter unfair or abusive practices from privileged access and control of data by more dominant countries in the region. In addition, since Africa's relatively small economic size and fragmented digital market represents a major constraint to digitalization, a common regional stance on data policies will vastly reduce these constraints and facilitate joint policy actions towards promoting digital development and unified influence on the global stage.
- ✓ Reduces cost and capacity limitations at the national level: A regional approach to data governance provides a more focused implementation strategy and a common pool of practical knowledge on best practices that every member country can leverage. Further, there will be better coordination of research into finding tangible solutions to risks associated with data sharing which would allow for economies of scale. Such approach will lower costs, and achieve greater benefits.

2.5 LESSONS FROM ATTEMPTS AT STRENGTHENING DATA GOVERNANCE

Among our stakeholder respondents, we find that the proposal for a regional data governance strategy is widely believed to be a good action plan. Nevertheless, they expressed their concern that actualizing such a plan is not without its antecedent hurdles. A review of past data regulation initiatives therefore provides lessons on constraints that need to be taken into consideration for future initiatives to succeed. Some of these lessons include:

- ✓ Priority level attached to data governance as development agenda needs to be similar and aligned across countries.
- ✓ Laws do not operate in a vacuum, therefore, transformation of data ecosystems in respect of legislation, enforcement, infrastructure, capacity development and resource allocation all need to happen concurrently.
- ✓ Transparency is required in negotiations/dialogue phase to address issues on what exactly a harmonized strategy would entail, and measures to be adopted in ensuring that there is no infringement on the sovereignty of any member country.
- ✓ Strong political will and commitment from all member countries to act upon the agreed strategy.

3.1 OVERVIEW OF THE AFCFTA AND RELEVANCE OF DATA GOVERNANCE IN TRADE AGREEMENTS

Africa's economic relations and interconnectedness have reached a critical juncture with the commencement of the AfCFTA. The AfCFTA initiative is part of the African Union's Agenda 2063 to transform the fortunes of Africa and upgrade the continent's status to becoming a global player. This newly formed single market assented to by 54 African nations with a population size of over one billion people, has the potential to facilitate unprecedented growth in African economies by solving the historically low level of intra-continental trade through elimination of tariff and non-tariff barriers to trade among member countries, and attract long-term stable investments from across the world. A significantly larger market could encourage growth opportunities for small and medium-sized enterprises which can translate to faster job creation. The AfCFTA agreement therefore seeks to address policy areas that will facilitate unhindered flow of goods/services, human resources, capital and investments across the region. With the AfCFTA now in full force, intra-African trade is forecasted to triple within a few years.

The AfCFTA's implementation mechanism is anchored on five operational instruments:

- i) *Rules of origin*: laid down criteria for exports to be considered as originating within the free trade area.
- ii) *Online negotiating forum*: virtual meetings by representatives of member states to facilitate discussions on subsequent protocols
- iii) *Monitoring and elimination of non-tariff barriers*: a regional online platform for report and tracking of progress on removing trade barriers not directly caused by tariffs.
- iv) *Digital payments system*: setting up a central pan-African payments and settlements system for processing, clearing and settling payments linked to intra-African trade.
- v) *African trade observatory*: a digital dashboard of trade statistics and information to aid comparisons across countries, guide market participants and track advancement in trade integration.

While most of the above structures are still in the formative phase, it is apparent that digitalization is crucial to the achievement of the AfCFTA (ODI, 2021) as it is the bedrock for executing the provisions of the pact, and monitoring progress. Easier and speedy sourcing of business finance, skilled personnel, suppliers, potential customers, and product delivery partners, are just a few examples of additional benefits of digital technologies in today's trade ecosystem. However, digital networks are largely dependent on data flow and analytics to improve efficiency and innovations for scaling up operations and broadening market penetration. E-commerce activities in particular are underpinned by data exchange by market players across borders. Governments are therefore justifiably concerned about protecting the integrity of their national data and security, and preserving citizens' rights to retain control over their personal information.

Data risks associated with e-commerce go beyond privacy breach. Due to the economic value of data as an intangible capital asset, privileged access and control over data can influence firm-wide and national competitive advantage. Inadequate data regulation can therefore create undesirable market outcomes, hence, the need to address data governance issues when negotiating trade agreements to ensure fairness and non-discriminatory treatment. Trade negotiators are invariably interested in including and agreeing on provisions to clarify rules governing the handling of data for trade purposes. This helps resolve questions on data ownership; parties permitted to process and extract intelligence from data; where information gathered should be processed and stored; who can use and leverage digital intelligence gathered, attribution of value

created from such intelligence; and if data can be transmitted freely between contracting countries or preconditions need to be met.

In the context of the AfCFTA, even though there is a general optimism surrounding its promise of economic development and increased prosperity for the region, there are still necessary building blocks that must be strengthened for it to succeed and benefit all Africans. One of such foundations is the need to fix gaps in policies, institutions, and structures to harness the potential of digital trade.

3.2 ROLE OF THE AfCFTA IN HARMONIZING DATA GOVERNANCE

One of the envisaged implications of the projected growth in intra-African trade spurred by the AfCFTA is increased data sharing across member countries. As African countries are beginning to develop policies governing data, there is an increased risk of incoherence and inconsistency of provisions across the continent. This can exacerbate the difficulties and challenges for African e-commerce businesses as they expand across borders within the continent. The AfCFTA therefore has a dual role as beneficiary and enabler of effective and harmonized data governance. Being a binding agreement on members, it could make enforcement of agreed data governance rules more manageable.

In the subsisting AfCFTA negotiations, there is no specific protocol / regional position on data governance and cross-border data transfers currently in force, other than a clause contained in Article 15(c)(ii) of the Protocol on Trade in Services. The article is not detailed in scope; simply an exception that permits member states to adopt necessary national measures to protect data privacy of its citizens as long as it is not implemented as a disguised means for restricting cross-border trade. Nonetheless, the next phase of the AfCFTA negotiations is expected to cover discussions on e-commerce protocol, which will include some components of data governance provisions. The plan is to conclude negotiations by the end of 2021. Substantive guidelines for negotiating the AfCFTA e-commerce protocol have not been released, however, given that discussion on the e-commerce protocol was fast tracked, it underscores the importance that the African Union attributes to building confidence in digital trade. It is imperative that extensive thought is given to the broad range of data policy issues in the e-commerce protocol. We highlight below, some data governance issues that need to be addressed:

- ✓ definition, scope of coverage, and regional stance on data governance
- ✓ rules for promoting seamless interoperability of cross-border data flows in a secure manner
- ✓ minimum standards on ethical use of data
- ✓ coordinated cybercrime laws, procedures for conducting investigations into reports, and intelligence sharing
- ✓ coordinated approach on taxing borderless transactions concluded through digital channels
- ✓ online consumer protections laws
- ✓ regulation of cross border payments various across African currencies and digital currencies
- ✓ principles on data protection, data security and privacy
- ✓ regulation on how open government data can be accessed
- ✓ management of digital identities
- ✓ data localization exceptions

While the AfCFTA may not provide room for resolving all the data governance challenges on the continent, its prominent role allows for substantial influence and better coordination of economic issues.

4.1 CONCLUSION

The digital revolution and data explosion across the globe has necessitated stronger data governance efforts. A robust data governance framework fosters good use of information, through rules, regulations, and policies that establish controls to ensure security, accountability, and trust. Increased data flows across borders add another level of complexity to data governance and demand greater action to ensure the protection and ethical use of data, especially citizens' data when being collected, processed, and used.

Based on our preliminary findings, we observe that national data governance efforts in Africa are developing at a slow pace and lack uniformity in approach. Although the degree of policy gap varies across different member countries, a more disturbing discovery is the inadequate implementation strategies in place. Reliable institutions and resources to support a well-functioning data governance environment are lacking in most African countries. The actualization of the AfCFTA's goals for an integrated and digitally connected Africa could therefore suffer without some support at the regional level. A regional approach to data governance is likely to yield faster results by building upon lessons from previous regional efforts and leveraging the enforcement and structural advantages of the AfCFTA.

This study does not envisage that the design of a regional data governance framework will be an easy task as there are challenges that need to be surmounted. Nevertheless, the hope is that with increased awareness and collaboration of all stakeholders in finding a workable solution to these issues, Africa's data governance can be strengthened to provide a conducive environment for the digital economy to thrive, by engendering trust and confidence in data systems.

4.2 AREAS FOR FURTHER INVESTIGATION

The findings made so far are beneficial in scoping focal areas for future studies in Africa as several unanswered questions remain. For instance, what is the level of citizens' awareness of inherent risks in data sharing and their rights to data privacy, and how does this explain their involvement in pressurizing governments to implement more effective data regulations? Also, what is the scope of coverage and applicability of existing data governance laws? Further, it is useful to evaluate how well national data governance strategies are embedded in and integrated with wider cross cutting digital development initiatives. To improve capacity for implementation and enforcement of data policies, it is important to examine the magnitude of technical/skills gap of policy makers and regulators in particular, investigate if funding of data protection authorities is sufficient and if not, what are the alternative revenue mobilization avenues. In addition, assessing the practical challenges that hinder a regional harmonized data framework could elucidate possible solutions.

References

Ademuyiwa, I. & Adeniran, A., 2020. *Assessing Digitalization and Data Governance Issues in Africa*, Ontario: CIGI Paper No. 244.

African Declaration on Internet Rights and Freedoms. African Internet Rights, https://afrisig.org/wp-content/uploads/sites/2/2017/11/African-Declaration-on-Internet-Rights-and-Freedoms_AfriSIG2017.pdf. Accessed on 13 May 2021

African Union Convention on Cyber Security and Personal Data Protection. African Union, 27 Jun 2014, https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf. Accessed on 13 May 2021

African Union Development Agency - NEPAD, 2020. *Cybersecurity Assessment Report*, South Africa: s.n.

Agreement Establishing The African Continental Free Trade Area. African Continental Free Trade Agreement, 21 Mar 2018, https://au.int/sites/default/files/treaties/36437-treaty-consolidated_text_on_cfta_-_en.pdf. Accessed on 11 May 2021

Altman, S. & Philip, B., 2020. DHL Global Interconnectedness Index: The State of Globalization in a Distancing World. <https://www.dhl.com/content/dam/dhl/global/dhl-spotlight/documents/pdf/spotlight-g04-global-connectedness-index-2020.pdf>. Accessed on 19 May 2021

Belle, J.-P.V. et al., 2018. *Africa Data Revolution Report: Status And Emerging Impact Of Open Data In Africa*, Washington: World Wide Web Foundation.

CSEA, 2021. The Imperativeness of Data Governance In The AfCFTA <http://cseafrica.org/the-imperativeness-of-data-governance-in-the-afcfta/>. Accessed on 17 May 2021

Data protection around the world. Commission Nationale de l'Informatique et des Libertés, <https://www.cnil.fr/en/data-protection-around-the-world>. Accessed on 12 May 2021

Declaration of Principles on Freedom of Expression. African Commission on Human and Peoples' Rights, 23 Oct 2002, <http://hrlibrary.umn.edu/achpr/expressionfreedomdec.html>. Accessed on 13 May 2021

Economic Commission for Africa, 2021. *Imperative for expediting African Continental Free Trade Area negotiations on e-commerce*, Addis Ababa: United Nations Economic Commission for Africa.

Gonçalves, P. V. R., 2020. Data governance. [Online] Available at: <https://dig.watch/issues/data-governance>

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Organisation for Economic Co-operation and Development, 23 September 1980, <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm>. Accessed on 14 May 2021

GSMA, 2021. Africa's Data Opportunity? Cross-Border Data Flows and IoT. <https://www.gsma.com/publicpolicy/wp-content/uploads/2021/01/Africas-Data-Opportunity-Cross-Border-Data-Flows-and-IoT-Webinar-Slides.pdf>. Accessed on 19 May 2021

IFC, 2020. *E-Economy Africa 2020: Africa's \$180 billion Internet economy future*, Washington: International Finance Corporation/Google/Accenture.

Ilori, T., 2020. *Data Protection In Africa And The Covid-19 Pandemic: Old Problems, New Challenges And Multistakeholder Solutions*, s.l.: Afriican Declaration on Internet Rights and Freedoms.

- Lexi, N. 2019. Data Localization Laws are Making African Trade Less Free. <https://weetracker.com/2019/09/20/data-localization-laws-are-making-african-trade-less-free/>. Accessed on 19 May 2021
- Macmillan, R., 2020. *Data Governance: Towards a Policy Framework*, Johannesburg: Centre for Competition, Regulation & Economic Development (CCRED).
- Resolution on the Right to Freedom of Information and Expression on the Internet in Africa*. African Commission on Human and Peoples' Rights, 4 Nov 2016, <https://www.achpr.org/sessions/resolutions?id=374> Accessed on 14 May 2021
- ODI, 2021. *E-commerce in preferential trade agreements: Implications for African firms and the AfCFTA*, London: Overseas Development Institute.
- Orrel, T., 2015. *THE AFRICAN DECLARATION ON INTERNET RIGHTS AND FREEDOMS: A Positive Agenda for Human Rights Online*, London: Global Partners Digital.
- Oxford Business Group, 2020. Benefits of the African Continental Free Trade Area agreement. <https://oxfordbusinessgroup.com/analysis/game-changer-new-trade-deal-lays-groundwork-acceleration-integration-and-intra-0>. Accessed on 17 May 2021
- Sacks, S. & Sherman, J., 2019. *Global Data Governance: Concepts, Obstacles, and Prospects*, Washington: new America.
- SMA, 2021. *Africa's Data Opportunity? Cross-Border Data Flows and IoT*, Nairobi: GSMA.
- UNCTAD, 2018. Economic Development in Africa Report, New York. https://unctad.org/system/files/official-document/aldcafrica2018_en.pdf. Accessed on 19 May 2021
- UNCTAD, 2019. E-commerce holds huge promise for enhancing free trade in Africa. <https://unctad.org/news/e-commerce-holds-huge-promise-enhancing-free-trade-africa>. Accessed on 17 May 2021
- UNCTAD, 2019. *Digital Economy Report - Value Creation and Capture: Implications for Developing Countries*, Geneva: UNCTAD.
- UNECA, 2019. *Next steps for the African Continental Free Trade Area*, Addis Ababa: United Nations Economic Commission for Africa, African Union, African Development Bank and United Nations Conference on Trade and Development.
- World Bank 2020. The African Continental Free Trade Area. <https://www.worldbank.org/en/topic/trade/publication/the-african-continental-free-trade-area>. Accessed on 18 May 2021

APPENDICES

1 Overview of data governance legislation in Africa by country*

S/N	Country	Electronic Transactions Laws	Cybercrime Laws	Consumer Protection Laws	Privacy & Data Protection Laws	No. of sub-indices ticked
1	Algeria	✓	✓	✓	✓	4✓
2	Benin	✓	✓	✓	✓	4✓
3	Cabo Verde	✓	✓	✓	✓	4✓
4	Comoros	✓	✓	✓	✓	4✓
5	Cote d'Ivoire	✓	✓	✓	✓	4✓
6	The Gambia	✓	✓	✓	✓	4✓
7	Ghana	✓	✓	✓	✓	4✓
8	Kenya	✓	✓	✓	✓	4✓
9	Libya	✓	✓	✓	✓	4✓
10	Madagascar	✓	✓	✓	✓	4✓
11	Morocco	✓	✓	✓	✓	4✓
12	Niger	✓	✓	✓	✓	4✓
13	Senegal	✓	✓	✓	✓	4✓
14	South Africa	✓	✓	✓	✓	4✓
15	Zambia	✓	✓	✓	✓	4✓
16	Egypt	✓	✓	✓	✓	4✓
17	Uganda	✓	✓	✓	✓	4✓
18	Cameroon	✓	✓	✓	×	3✓
19	Malawi	✓	✓	✓	×	3✓
20	Rwanda	✓	✓	✓	×	3✓
21	Seychelles	✓	✓	✓	×	3✓
22	Tanzania	✓	✓	✓	×	3✓
23	Angola	✓	✓	×	✓	3✓
24	Burkina Faso	✓	✓	×	✓	3✓
25	Guinea	✓	✓	×	✓	3✓
26	Mali	✓	✓	×	✓	3✓
27	Mauritania	✓	✓	×	✓	3✓
28	Mauritius	✓	✓	×	✓	3✓
29	Togo	✓	✓	×	✓	3✓
30	Tunisia	✓	×	✓	✓	3✓
31	Nigeria		✓	✓	✓	3✓
32	Botswana	✓	✓	×	×	2✓
33	Ethiopia	✓	✓	×	×	2✓
34	Sudan	✓	✓	×	×	2✓
35	Mozambique	✓	✓	×	×	2✓
36	Liberia	✓	×	✓	×	2✓
37	Sierra Leone	×	✓	✓	×	2✓
38	Lesotho	×	✓	×	✓	2✓
39	Sao Tome and Principe	×	✓	×	✓	2✓
40	Guinea-Bissau	×	×	✓	×	1✓
41	Chad	×	×	×	✓	1✓
42	Democratic Republic of Congo	×	×	×	✓	1✓
43	Equatorial Guinea	×	×	×	✓	1✓
44	Gabon	×	×	×	✓	1✓
45	Burundi	×	✓	×	×	1✓
46	Djibouti	×	✓	×	×	1✓

S/N	Country	Electronic Transactions Laws	Cybercrime Laws	Consumer Protection Laws	Privacy & Data Protection Laws	No. of sub-indices ticked
47	South Sudan	×	✓	×	×	1✓
48	Zimbabwe	×	✓	×	×	1✓
49	Central Africa Republic	×	×	×	×	0
50	Congo Republic	×	×	×	×	0
51	Eritrea	×	×	×	×	0
52	Namibia	×	×	×	×	0
53	Saharawi Arab Democratic Republic	×	×	×	×	0
54	Somalia	×	×	×	×	0
55	Swaziland	×	×	×	×	0

* Legislation in force as at the time of this report, based on available information per UNCTAD's cyber law tracker and sourced from official data protect authorities' websites.

2 Summary of Stakeholder Consultations

A. Interviews were conducted with 16 stakeholder organizations with operations covering West, East, and Southern Africa regions. Organization type is provided below:

1 – Data aggregator
2 – Government agencies
2 – Multilateral organizations
11 – Civil society including digital rights and internet affordability advocates, research institutes, etc.

B. Rank what the top priorities that policy makers on data governance should focus on?

- ✓ Capacity for better implementation – this includes setting up independent data governance agencies and equipping them with adequate skilled manpower, technical training and other resources
- ✓ Legislation on data protection and processes for data collection and accessibility, to prevent human right violations
- ✓ Enabling infrastructure to drive digital inclusion

C. Any potential impact on the perception of the importance of data governance as a result of Covid-19 and the AfCFTA?

- ✓ Yes – 2/3 of respondents

D. Are current data governance policies adequate in the countries you operate in?

No – about half of the respondents. About 20% responded in the affirmative, and insist that the issue is not lack of policies, but rather implementation, Others, especially those from East Africa hinted their laws are relatively new so too early to assess,

E. How effective are domestic data governance institutions?

- ✓ Not effective – majority responses

F. Major challenges faced by data governance institutions?

- ✓ Lack of technical digital and data skills
- ✓ Funding

G. Major benefits and challenges embedded in a regional data governance approach in Africa?

Benefits - Harmonization and coordination

Challenges - Difficulty in getting all countries to align their objectives, inadequate existing structures in implementing countries and bureaucracy in AU's processes.

H. General suggestions and advice to improve projective outcome?

- ✓ Recognize that data governance issues go beyond law, it involves technical resources, human resources, etc. and it is important to have a system that brings it all together.
- ✓ There needs to be a lot more action towards citizen awareness and improving citizen pressure on the issue.
- ✓ Expose the tangible risks associated with ineffective data governance so policy makers can appreciate the importance and drive change
- ✓ Collaborate with pan-African coalitions working on similar objectives



-  @csea_Afric
-  @csea-africa
-  @Cseaafrica
-  Enquiries@cseaafrica.org
-  234-9-291-4822, +234-9-291-4820
-  No 4 dep Street off Danube crescent
Maitama – Abuja, Nigeria
-  www.cseaafrica.org