CSEA
Centre for the Study of the Economies of Africa

STRENGTHENING DATA SHARING PRACTICES IN AFRICA

RECOMMENDATIONS FOR RESPONSIBLE DATA GOVERNANCE AND ECONOMIC DEVELOPMENT

Author: Kunle Balogun

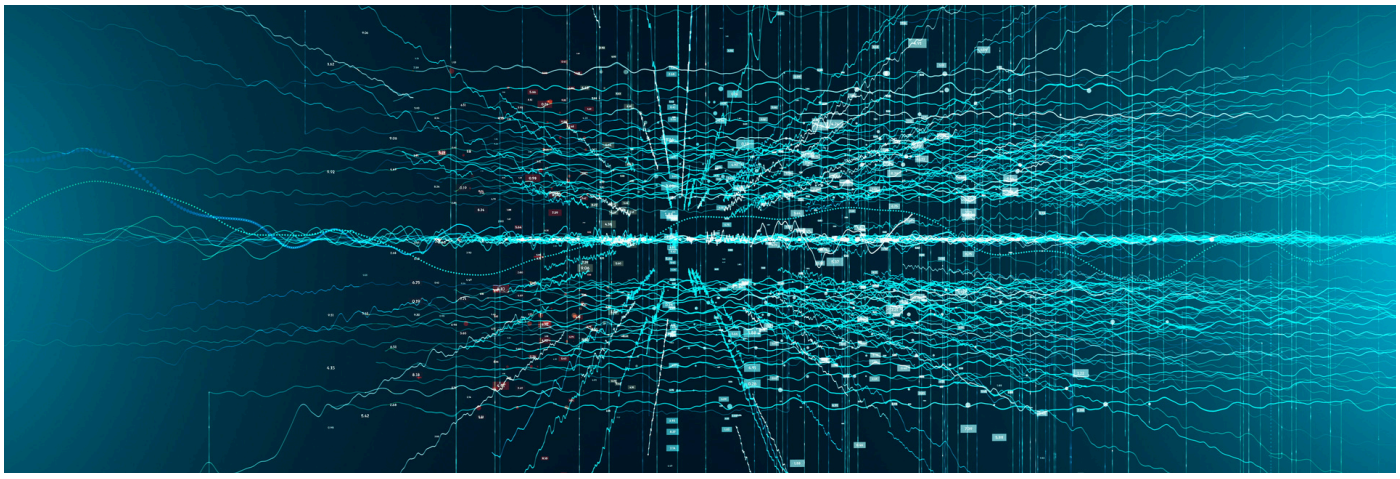
www.cseaafrica.org

Background

In Africa, the digital economy, which refers to all economic activities facilitated by digital technologies and big data, is booming. This is a result of digital technology's capability to transform economies and societies, influencing how we work, live, and interact. Africa's digital economy is a boost to the continent's economy. International Finance Corporation (2020) reveals that Africa's digital economy grew from $100 billion to $115 billion, representing a 15% increase between 2019 and 2020. It further projects that Africa's digital economy has the potential to contribute $180 billion and $712 billion to the continent's gross domestic product (GDP) by 2025 and 2050, respectively.

The role of data, in the public and private sectors, is central to informing strategy, shaping decision and policy-making, creating value, driving innovation, sustaining profit-making and promoting economic development.

Constituting an integral part of the data value chain, data sharing promises many opportunities to people across the globe by boosting digitalisation, creating jobs, and raising standards of living. In Africa, data sharing in diverse sectors has the potential to ensure economic benefits for the continent; hence, no effort is spared to ensure that it is well governed to be effective and productive for the continent's good. In the field of science, for instance, data sharing helps boost the cross-fertilisation of scientific ideas that can facilitate the continent's scientific development. Hence, the coordinated approach towards strengthening the governance of data-sharing practices in the field constitutes an important perspective to emerging debates. Also, on the economic front, cross-border data sharing is a key factor for promoting national and regional trade in Africa. It is a great enabler for the African Union's realisation of the benefits of the African Continent Free Trade Area (AfCFTA), an intra-Africa trade that is aimed at boosting the continent's digital economy.



However, data-sharing practices across the diverse sectors in Africa are obviously in constrained circumstances, as they are confronted by many challenges which stifle their capabilities to deliver the most benefits for the continent's economic growth and development. This policy brief addresses some of such challenges that militate against data-sharing practices in Africa as well as recommends some effective data governance measures that can boost the continent's digital economy towards economic transformation and development.

Data sharing practice-related challenges in Africa

Data Leakage

Data leakage is an emerging issue of concern for Africa's data governance ecosystem, which occurs when sensitive or proprietary data (information) is informally shared from the continent with the outside world. This implies that there is cross-border data sharing but in an informal process. The large proportion of data in diverse sectors like finance, academic, health, legal, and telecommunication that leaks out of the African continent's data space via electronic media could be legal or illegal. It is legal when data is shared across the continent's border for a particular purpose, but it may eventually be processed or used for other purposes entirely different from the original intent. On the other hand, illegal data leakage refers to any data leakage through a maliciously intentional or premeditated process.

Legal data leakage on the continent could be illustrated with the raw personal medical data collected by radiologists through the aid of the Mental Resonance Imaging (MRI) scan machine. But contrary to the sharing of mutual benefits that both Africa and the rest of the world should enjoy in the data space, much of Africa's medical dataset, like the MRI scan data that is sent out of the continent for interpretation, is often exploited by the technologically advanced nations (to which it is sent) to their economic advantage. Conversely, the illegal data leakage is best illustrated by the unethical collection of data by proxies from the continent, where data collectors fail to properly identify the true destination of the collected data. Data leakage, which could be attributed to certain factors, has negative consequences on the continent, including but not limited to loss of potential for innovation, negative implications for long-term economic growth and development, and limitation of technological and technical knowledge transfer.

Data privacy and protection compromise

The African digital economy is largely threatened by data privacy and protection compromise which robs the continent of huge economic benefits. Africa's data-sharing system is imperilled by data privacy and protection issues, which include data breach, surveillance and identity theft, among others, thus posing a serious threat to data-sharing practices both within and outside the continent. According to Interpol's Africa Cyber threat Assessment Report (2021), data breaches cost African economies nearly $4 billion annually.

Poor/low data quality

Poor data quality manifests when the shared data contains errors and inconsistencies, probably due to faulty data-sharing mechanisms or poor processing due to infrastructure and capacity gaps. There is evidence that most of the data that is collected from the continent is in a format that defies machine readability. The sharing of poor and low-quality data in Africa is currently a subject of concern, especially against the urgent need for quality and reliable data, which is necessary for accelerating the continent's development.

Lack or loss of data control

In Africa, lack or loss of data control is considered a major challenge for data sharing, especially in relation to both organisations and individuals. Except specific data stewardship and processing or provisions are in place, most of the data shared usually moves outside the data system of the original data holder (data controller), hence, out of his or her control. The same applies to data subjects who provide their data and give their consent for their re-use and sharing but, thereafter, lose their capabilities to control how their data is re-used.

Restrictive data localisation and sovereignty policies

The benefits that data-sharing practices in Africa promise are limited by data localisation requirements, which restrict data flow from one country or data jurisdiction to another. Such restrictions in Africa raise the cost of doing business across borders, thus robbing the continent's digital economy of economic opportunities. Often, data sharing across borders, like the earlier mentioned MRI scan data, should be deemed beneficial when the purpose is to process the data, similar to crude oil, to create value. Restricting such could invariably have side effects for the continent. It is instructive to note that good data governance does not consist of imposing restrictions on data generally, as such an approach could throttle data-driven innovation.

Factors responsible for these challenges

Lack of internal processing capacity

The medical data leakage case cited earlier is attributed to the continent's lack of human capacity and the necessary data processing infrastructure required to process the data and extract its inherent value. Records show that most African medical facilities lack the capacity to interpret MRI scan results, which is why such results are typically sent out of the continent for interpretation. Given its versatility in the management of non-communicable diseases (NCDs), Magnetic Resonance Imaging (MRI) has had significant growth in its use across the globe since its inception in the 1970s. Notwithstanding, in certain regions with limited resources, like Africa, MRI availability and use are apparently limited by high acquisition and maintenance costs, limited access to the infrastructure, and lack of expertise required to run and maintain the equipment.

Weak data governance around cross-border data flow process

Weak or absent data governance structures in most African countries strongly contribute to the porous cross-border data-sharing system. When the enactment of data protection laws and regulations is not consciously matched with strict compliance and enforcement, data is definitely at risk of vulnerabilities at any of the sharing and processing stages. The case of the Nigerian SIM card registration data leak, in which multiple instances of SIM card registration data were compromised and sold on the black market, is reportedly linked to the lack of robust cyber security practices, stringent data protection regulations, and effective enforcement mechanisms in the country.

Knowledge gap between data policy formulation and implementation

Another responsible factor is the manifest knowledge gap that exists between the formulation of data policies and standards and the implementation of such. In most African countries, while there are relevant institutions (at the continental, regional and national levels) with the statutory responsibility to formulate data-related policies and standards, there are also those in whom power is vested in coordinating the implementation of such policies and standards. However, while a good number of promising standards and policies have been formulated for effective data management which can help stave off possible data vulnerabilities, findings establish that the problem essentially lies in the implementation of such.

Power imbalances/inequalities

Within the context of global data value chains, whereby different stages of data collection, storage, analysis and processing largely take place between countries or continents, there is growing awareness that cross-border data flows are imbalanced. This is not unconnected with the reality that there is a huge concentration, in a limited number of developed countries (like the European Union, the US and China), of such data firms that have comparatively higher power and adequate resources to process data and thereby create innovative value out of it in the data-driven digital economy. Clearly, these foreign firms capture most of the gains from data shared across borders. Compared to their developing counterparts like most African countries, these developed countries are clearly leading digital powers in terms of their higher level of digital preparedness. However, it is noteworthy that very few digital leaders are emerging in a limited number of developing countries like India, Indonesia and South Africa.

Recommendations for responsibly governed data sharing practices

Bridging the capacity and infrastructure gaps in the continent's data ecosystem: Today, Africa is facing a significant shortage of data professionals and lacks the necessary processes for extracting data value. This is what largely informs the outflow of data to where value can be extracted from it. Consequently, to enable the continent to effectively manage data generated by its people and industries and, more importantly, maximise its value, there is a need for strategic investment in data vis-à-vis the development of both human and infrastructure capacities. Aside from its capability to create an enabling and trusted environment that mitigates data-associated risks, this intervention will create opportunities for the continent in the areas of digital equity, inclusion and entrepreneurship.

Embedding ethical considerations into data governance practices: One of the important requirements for strengthening the continent's data-sharing system is adherence to certain ethical standards that can help shape data management policies. It is proper to embed ethical considerations into data governance practices that align with best data-sharing practices, where data collection and sharing processes adhere strictly to the principles of informed consent, fairness, honesty, transparency, accountability and openness. Data collectors are required to maintain all these principles in their collection, storage, use, or sharing of individuals' data. For instance, obtaining individuals' informed consent relates to managing their consent for the collection, processing, use and or sharing of their personal data. It involves providing detailed, clear and accessible information to individuals about the purpose and nature of the data processing, and their rights regarding their personal information. This shows the centrality of trust to the various dimensions of data governance.

Trust, in this context, does not refer to data accuracy but to fairness, honesty, transparency, accountability and openness on the part of the numerous systems that collect, use and share data. Data collectors should be compelled to owe a sort of fiduciary duty of loyalty to data subjects regarding managing their (data subjects') personal data. This measure will discourage the unhealthy practice whereby most data collectors on the continent throw ethics to the wind by failing to properly give details about the true destination or recipient of the data they collect, thereby encouraging data leakage.

Strengthening the continent's cross-border data flow regulations: The globally emerging discourse around data governance shows that Africa's position in this space is yet to be properly defined, given its weak state of digital governance framework required to effectively manage its cross-border data flows. This development has, for long, robbed the continent of the many benefits of digitalisation, the most of which are socio-economic development. For the African continent to have a well-regulated cross-border data flow regime that can safeguard data from any data sharing vulnerability, which can consequently compromise its usability, integrity, quality and security, all the key actors in its data governance ecosystem must collaborate to strengthen its cross-border flow regulations. Measures must be implemented to ensure the enforcement of and compliance with such regulations.

Furthermore, to ensure effective enforcement and compliance, all relevant data governance institutions must develop the mechanism of regularly inspecting all public and private entities involved in the data governance ecosystem. They should also closely monitor the continent's compliance with data protection obligations under international conventions and agreements. More importantly, it is worth adding that Africa's regulatory approach towards managing cross-border data flows must be designed in a way that facilitates a kind of reciprocity or win-win deal, whereby the benefits of data (private or public) can be productively maximised to the mutual advantage of the continent and the global digital powers that are better equipped to extract value from data. This implies that if our data is taken or leaked to the US, China or India, we, as data providers, should also benefit. If our data is used to extract value, it shouldn't be commoditised exorbitantly for us. Also, the development whereby some institutions come to Africa and collect some statistical data freely must redound to economic benefits for us as a continent.

Rethinking the continent's data localisation policy for equitable distribution of data values or benefits: The existing power imbalance that characterises cross-border data-sharing practices in the global data space is largely considered a justification for most African countries to adopt stringent policy measures like data localisation whereby they keep their data within their jurisdiction/boundaries. To such countries, cross-border data sharing cannot be beneficial as long as only a few global digital corporations from a few developed countries continue to capture most of the gains from the data flows.

It is, however, important to consider that, while on the one hand, there cannot be value without the raw data, on the other hand, having access to the data without the internal capacity to process and monetise it or to create social value out of it is clearly of no use. As a matter of fact, imposing restrictions on cross-border data flows, which creates barriers and uncertainty for firms and individuals seeking to exchange data across borders, may not be economically wise for the African continent.

- ***Fostering international data collaboration/cooperation with global digital powers:*** The absence of strategic international data collaboration or cooperation among most countries of the world makes all cases of data sharing issues a serious cause for concern, especially in vulnerable data spaces like Africa, where a strong data governance regime that could prevent such is just evolving. Since data can cross borders, the African continent must collaborate with global digital partners to address various vulnerabilities and share best practices in data governance. This collaboration can ensure the collective realisation of the benefits that data can offer at the global, continental, regional and national levels More importantly since Africa does not currently have the adequate capacity to extract value from its data and developing such capacity remains a long-term effort, data collaboration, rather than the much-talked about data localisation, seems to be the continent's immediate need.

- ***Implementing robust data security measures:*** To protect digital data, such as official statistical data, from vulnerabilities like data leakage, robust data security measures must be implemented. To achieve this, encryption and authentication protocols could be used to secure data transmission and storage, and security assessments, vulnerability testing, and incident response planning could be regularly conducted.

Conclusion

Laying a strong foundation for healthy data-sharing practices in Africa requires that the continent devise an effective data governance framework that promotes trust and, at the same time, maximises the value of data. Since data governance involves the establishment of principles that enable an environment for the sharing of data, Africa must adopt proactive measures that make data sharing beneficial, improving living standards and boosting its digital market. These measures include devising an informed consent strategy in line with best data practices, implementing robust data security measures and fostering strategic data collaborations with global digital leaders to maximize the diverse benefits that healthy data-sharing practices can provide. The continent would do well by developing a strong data governance framework that effectively addresses the risks inherent in the nature of data while, at the same time, ensuring that a wide variety of its data can be leavened with a value that can be exploited to its greatest socio-economic advantage.