Symposium on the Economic Impacts of Data Localisation in Africa: Introduction

By:

Fola Adeleke

May 10, 2022

In January 2021, with the increase in the devastating economic impact of the COVID-19 pandemic, the Nigerian government launched the Rapid Response Register (RRR) for COVID-19 cash transfers the platform of the National Social Safety Nets Project (NASSP), funded by the World Bank. According to the Vice President of Nigeria during the launch of this programme, 'the RRR is designed to focus mainly on the urban poor wards selected using scientifically validated methods of satellite remote sensing technology, machine learning algorithm and big data analysis.' The RRR uses poverty maps, which show the communities in which poor people live and can substantially improve geographic targeting to help extend social protection. According to the World Bank, 'recent advances in deep learning were used to construct a high-resolution poverty map from satellite imagery and other sources of geospatial Big Data and 'these techniques work by being exposed to a large dataset that matches ground-truth labels of poverty (from geo-located household surveys)

to imagery and other geospatial data.' Nigeria's embrace of big data in rapidly expanding its social protection programme is one example of how African governments are maximising the promise of big data to achieve their governance objectives. On a different front in Kenya, big data is being used for sinister purposes by fintech firms that reveal how unregulated use of big data can have devastating economic consequences. Kenya is Africa's fintech pioneer with the invention of mobile money. With the increase of fintech firms providing instant access to microcredit to millions of Kenya, we are witnessing millions of Kenyans increasingly becoming over-indebted and stuck in a cycle of poverty. As Emma Park puts Kenya's new experience of debt, 'Kenyans are being driven into circuits of financial capital that are premised not—as the marketing would have it—on empowerment, but on the profitability of perpetual debt.' Fintech's primary financial product in Africa, mobile lending, uses algorithms to mine people's devices to assess their creditworthiness. The discriminatory impact of data mining by fintech companies is enormous. As Pascale, the author of The Black Box Society puts it, 'you can get in a death spiral simply by making one wrong move, when algorithms amplify a bad data point and cause cascading effects.'

The examples I have provided involve the use of personal data but none of the examples require the personal data in question to be localised in the country of use before it can be processed. Yet, there is an increasing fixation on the need to regulate the cross-border flow of personal data for access, control and processing. In a rapidly changing digital economy, personal data has become the focal point of regulation by states in the race towards maximizing the potential of the digital economy. In some African states, these personal data protection laws and regulations limit the cross border flow of data with various unintended consequences. The limit of cross border flow of personal data is broadly referred to as data localisation and is often justified based on five main concerns. These include the protection of personal data, access to data by local law enforcement, ensuring national security, advancing local economic competitiveness and levelling the regulatory playing field. However, a closer look at these justifications reveal the impact of data localisation on free trade, increase in transaction costs and the efficiency of corporations, stifling of innovation, and hampering of economic growth. With global data flows raising global GDP, it is necessary to ask, what policy trade-offs are necessary to

balance the legitimate concerns of countries against the unintended consequences that the impact of data localisation causes? There are four issues relating to the economic impacts of data localisation that emerging regulation in Africa needs to address. These are data ownership and its value, competition, trade, and foreign direct investment.

Ownership and the creation of value in the data economy

One primary issue concerns the ownership and storage of data. In centring ownership and informed consent for processing of personal data, some African countries such as South Africa are proposing policies on state ownership of data. However, this is at odds with the nature of data and how value is created from data. Assigning a market value to an individual's personal data for purposes of asset valuation or ownership is difficult. The non-rivalrous nature of data means that at a technological level, first, data is infinitely usable. Second, the interconnectedness of data linking a subject's data with another makes it difficult to for example, separate and to claim exclusive ownership of personal data. Third, once personal data is in the public domain, they cannot be returned to the private control of their user. Consequently, deriving economic value from data is based on control of infrastructure for processing personal data. The control and cost of infrastructure development raises other issues related to the economic impacts on trade, investment and competition.

Trade

There are limited rules to govern digital trade under existing multilateral trade agreements. In the absence of a multilateral digital trade regulation, several countries including the EU bloc have filled the regulatory gap with data privacy regulation that imposes conditional and limited cross-border transfers of personal data. Others such as the United States have taken the position that barriers to data flows impede legitimate cross-border trade and that is trade protectionism. Most African countries have taken the former approach on conditional and limited cross-border transfers of personal data but from the assessment of the emerging policy positions in Nigeria, South Africa and Kenya considered under this project, there are worrying signs that *de facto* localisation practices are emerging. These examples are referenced in the forthcoming essays to be published in this symposium.

The relative homogeneity of Africa's data economies suggests it can leverage the opportunity of regional agreements to address some of the issues around data localisation. The African Continental Free Trade Area (AfCFTA) Agreement, which commits to eliminate all forms of barriers to trade and to promote movement of capital and natural persons, will soon adopt an e-Commerce Protocol that can provide uniform data protection and cross border data transfer rules without the need for restrictive data localisation regulation at a country level. Such Protocol should prohibit data localisation with narrow exceptions such as sensitive personal data that requires protection on grounds of national security. In addition, ratification of the African Union Convention on Cyber Security and Personal Data Protection, 2014 (Malabo Convention) which allows conditional transfers of data is necessary.

Investment

Several studies considered in our research show that data localisation rules increases the costs of doing business by foreign firms operating in various domestic markets. While some governments believe that data localisation requirements can boost their economies through forced foreign investment by global firms to build infrastructure such as data centres locally, such investments are expensive and risky. Such risks include energy insecurity and unpredictable regulation. While it is not always clear who will bear the additional costs associated with data localisation, one thing that is clear is that whatever additional costs result from data localisation, it will likely affect micro, small and medium-sized businesses disproportionately.

Competition

The propensity of data firms to become dominant in their market and to abuse their dominance is a cause for major concern for regulators. The ability of big firms to collect and process large sets of data allows market dominance that traditional competition regulation cannot easily regulate. One way of addressing the impact of data localisation on the competitiveness of firms is through data interoperability (the ability for different systems to share and use data in a coordinated, timely manner) or data sharing agreements (when two or more firms agree to merge their data for access by themselves and possibly third parties). This will require recognising data subjects' right to portability.

Harmonisation of competition regulation is also one way forward in addressing gaps in competition enforcement. The existing regional competition authorities in Africa such as the Common Market for Eastern and Southern Africa Competition Commission, the Economic Community of West African States Competition Authority and the East African Community Competition Authority can serve as the basis for integrating competition policy across the continent. In addition, new agreements such as the AfCFTA could also foster harmonization on competition policy for the data-driven economy through the competition policy protocol.

The question on policy trade-offs on data protection that this symposium wrestles with was examined through various themes with a focus on the applicable laws and regulation in Nigeria, South Africa, and Kenya. The first essay by Dr. Beyleveld introduces the regulatory implications of data protection in Africa. He describes the rise of the data economy as well as its characteristics, the omnipresent information asymmetries and the extent to which artificially intelligent machines and those that control them are far more capable of extracting value from massive amounts of raw data than human beings are. It also explores concepts around the rise of “winner-take-all” or “winner-take-most” markets and what this means for the competitiveness of markets; value creation in the data economy; the “digital divides” between and within countries and what these mean for the distribution of benefits in the data economy.

The second essay by Dr. van der Berg explores arguments around states’ justification for introducing data localisation requirements, including those related to foreign surveillance; privacy and security; and economic development. In addition, arguments that oppose “data nationalism” is explored, with reference to the unique challenges that confront South Africa’s policy makers, including a lack of ICT infrastructure and serious power constraints. In particular, the polycentric and sometimes perverse consequences that may result from data localisation is set out.

The third and fourth essays focus on country commitments in international treaty frameworks and the intersection with data protection. With the ratification of the Africa Continent Free Trade Agreement (AfCFTA), Africa has been turned into a single free trade area, however, leading African economies

including Nigeria and Kenya have adopted data localisation laws that could potentially hamper the success of trade in Africa's digital economy. The writers explore the national data regulation frameworks in Nigeria and Kenya and the interaction of these frameworks with the international commitments of each country, identifying a number of priority issues that states should take into account for future regulation and implementation. The contributors for Nigeria are Drs. Lukman Abdulrauf and Abe and for Kenya, Mr. Malcolm Kijirah and Ms Wangari Thuo.

The final essay in this symposium looks at the most frequently proffered rationales for data localisation, most of which seek to change the definitional contours of the economic characteristics of data, including through seeking to render it a rivalrous commodity, internalising privacy protection and rendering data completely excludable. We look forward to your engagement on these issues we raise.

View online: Symposium on the Economic Impacts of Data Localisation in Africa: Introduction

Provided by Afronomicslaw