Symposium on the Economic Impacts of Data Localisation in Africa: Personal Data Protection and Economic Integration: Options for AfCFTA Negotiators

By:

Alexander Beyleveld

May 12, 2022

Introduction

In February 2020, the Assembly of the African Union (AU) adopted a decision on the African Continental Free Trade Area (AfCFTA). Against the backdrop of the establishment of the AfCFTA through the conclusion of a first round of negotiations, which was to be followed up by a second round of negotiations on a number of additional issues, the Assembly decided – amongst other things – that there would be a third phase of negotiations focusing on an AfCFTA Protocol on E-Commerce. It was later announced that the Phase III negotiations would be fast-tracked and would take place alongside Phase II negotiations,

with the Assembly of the AU subsequently endorsing a decision taken by the African Ministers of Trade (AMOT) that both Phase II and III negotiations be completed by the end of 2021.

While the extent to which progress has been made on the AfCFTA e-commerce negotiations remains unclear to most observers, the importance of the issues it will likely address – especially those relating to data – is readily apparent. While commerce has always relied on information, 'data', as the term is understood today, goes well beyond mere information; by most estimates, moreover, data are also far more valuable than ever before. While many have noted that the value of data is difficult to measure, there are many ways to illustrate the point. A simple example comes from the astronomical growth of data-driven firms listed on stocks exchanges. As an Organisation for Economic Co-operation and Development (OECD) has illustrated, while the average data-driven firm listed on the New York Stock Exchange was worth around the same as the average firm for the exchange as a whole in terms of 1985 market capitalisation, the average data-driven firm was around ten times as valuable by 2020.

This rise of the data-driven economy should also be viewed against the backdrop of a number of distinct – but related – trends. Chief among these, perhaps, is what economist Richard Baldwin refers to as the 'Great Convergence', that is, the rapid economic growth in a significant number of emerging economies – led by the likes of China, South Korea and India – that far outstripped growth in richer, mostly Western countries, that led to a rapid reduction in the economic gap between the former and latter group of nations. The Great Convergence has, in turn, contributed to significant shifts in geopolitics and geoeconomics, shifts which are perhaps best illustrated by increased tensions between the United States and China. These shifts have contributed to what current Director General Ngozi Okonjo Iweala has called a ' stagnant and paralysed' World Trade Organization (WTO), the result being an ever increasing shift towards new trade rules being negotiated bilaterally or regionally in the context of so called preferential or free trade agreements (PTAs or FTAs) such as the AfCFTA.

Rules on cross-border data flows are no exception to this general trend. Moreover, given that the WTO rulebook was mostly written in the 1990s prior to the rise of the data driven economy, multilateral trade rules by and large do not

regulate cross-border data flows, a fact which has contributed to rules on this front – demand for which has only increased as economies have become more data intensive – being set nationally and even sub-nationally, but also regionally, and in PTAs and FTAs. At the same time, trends such as the rise of what is often referred to as 'surveillance capitalism' has brought the issue of personal data protection on privacy grounds into sharper focus around the world. With this background context in place, this essay looks at the intersection of economic integration and personal data protection with a view to informing ongoing debates on what AfCFTA rules on cross-border data flows might look like.[1]

Dominant Approaches to Regulating Cross-Border Data Flows and Personal Data Protection

While there is nothing preventing AfCFTA member states from adopting rules on cross border data flows and data protection which do not closely resemble those adopted elsewhere, even a completely integrated African economy – which we are still very far away from – would be relatively small compared to the economies of the United States (US), the European Union (EU) and China. For this and a number of additional reasons, it is important to understand what the dominant approaches to regulating cross-border data flows and data protection look like: African states of all shapes and sizes will be pressured by larger economies to adopt their own regulatory model and, regardless of whether countries acquiesce, the future economic relationships between AfCFTA member states and the rest of the world may well be shaped, at least partially, by the operation of these rules. The extent to which AfCFTA rules are compatible with US, EU and Chinese rules, moreover, will affect the level of integration between the continent and these economies – something which will be of great strategic importance as the level of continental integration increases in future.

The US Approach

US practice reflects the country's regulatory preference for 'free' cross-border data flows and a so called economic approach to the protection of personal information. This much is evident from its approach in FTAs and PTAs, including the Comprehensive and Progressive Agreement for Trans-Pacific Partnership

(CPTPP) – an agreement which the US no longer belongs to, but whose rules it was influential in shaping – the United States-Mexico-Canada Agreement (USMCA) and the US-Japan Digital Trade Agreement, as well as the stance it has taken in multilateral negotiations on e-commerce at the WTO. Ultimately, the general point of departure for the US is that cross-border flows of personal data shall not be prohibited or restricted. While the US approach does acknowledge the importance of data protection, allows for deviations from the general rule in exceptional circumstances, and provides guidance in relation to what constitutes 'exceptional circumstances', US-led regimes are generally very liberal vis-à-vis other regimes and are often viewed as favouring US tech giants.

The EU Approach

The EU approach is mostly embodied in the General Data Protection Regulation (GDPR), which, unlike the top-down economic approach adopted by the US, is a bottom up approach grounded instead in fundamental rights. The starting point in the EU is accordingly quite different. Unlike in the US case, the default is not that prohibitions or restrictions on data flows, including personal data flows, are not permitted. Instead, the EU approach, exemplified by the text it has proposed in relation to the conclusion of a trade agreement with Indonesia, seems to propose a closed list of instances when data flows shall not be restricted between the parties to an agreement, implying that all other restrictions are generally acceptable (with some leeway provided for adding additional items to what will remain a closed list). The EU approach is also far more concerned with ensuring that the GDPR does not come into conflict with trade rules. Its approach is thus far more privacy-oriented than the US approach, and far less liberal. It is still generally permissive (and even encouraging) of cross-border data flows, but it does allow parties to retain far greater regulatory control over the protection of personal data on privacy grounds.

The Chinese Approach

The Chinese approach has thus far been quite different. While there has been some limited provisions in Chinese trade agreements regarding the protection of personal information, China has thus far not made any commitments in relation to cross-border data flows, opting instead to use its domestic laws to

regulate both the protection of personal information and data flows. In terms of the Chinese Cybersecurity Law, China has set up an entirely different regime in that it requires data localisation in respect of certain data flowing into China, which both US and EU PTAs and FTAs seek to prohibit. Moreover, outflows of data are not permitted by default either. Instead, they are subject to an outbound 'security assessment'. The Chinese approach is accordingly the least liberal of the three dominant paradigms in the sense that it has yet to include or propose the inclusion of obligations that relate to data flows in its PTAs or FTAs. Yet, there is an emerging consensus that China has stricter data protection laws than in the US and that its approach to data protection is even converging with the far stricter EU approach – new Chinese data protection rules that recently became law are proof of this proposition.

Options for AfCFTA Negotiators

While it should be recalled that the AfCFTA is an intra Africa agreement, disparities in levels of development remain among African countries and so the development needs of AfCFTA member state – which often vary a great deal – should be taken into account not only vis-à-vis the likes of the US, EU and China, but also vis-à-vis one another. Against this backdrop, it is first of all worth noting that many AfCFTA member states have adopted domestic data protection laws, mostly in ways that follow the EU's bottom-up, fundamental rights based approach, but that very few so-called South South PTAs and FTAs include provisions on data protection. Should these sorts of provisions start to become more common place with time (which seems probable), then, negotiators may be tempted to follow the EU's approach to integration. That said, it is possible that taking such approach will not be feasible with AfCFTA member state agendas, especially given that an increasing number of African states are implementing (or at least contemplating implementing) data localisation laws, which the EU approach to integration seeks to ban.

It is possible, however, for AfCFTA countries to modify the EU approach in order to meet their own particular needs. They could do so, for example, by altering the items included on the EU's proposed positive list. In other words, instead of simply proposing that measures that relate to localisation and outright prohibitions on storage or processing be included on the list of impermissible restrictions, AfCFTA member states could add to and/or remove from their

proposed list various types of measures depending on their negotiated liberalisation preferences. They could also propose that a party's rules and safeguards for the protection of personal data and privacy, including on cross-border data transfers of personal data, should be subject to regulatory cooperation (whereas the EU approach suggest these rules and safeguards should not be subject to regulatory cooperation).

As for the US approach, it is worth pointing out that there is no reason that it cannot be implemented in a fashion that treats privacy as a fundamental right. This is especially the case if one adopts a modified version of the US approach whereby one expands the exceptional circumstances in which the general rule against prohibitions or restrictions on data flows does not apply. This would be similar to creating a negative list. In other words, AfCFTA member states could propose making it a general rule that data flows, including of personal data flows, should not be prohibited or restricted except for in specifically enumerated instances (as opposed to the US approach which merely provides a general exception). The US approach could also be adjusted in other ways, for example through strengthening its provision on the protection of personal information, for example through requiring compliance with other AU treaties, such as the African Union Convention on Cyber Security and Personal Data Protection.

The Chinese approach may be attractive from the perspective of countries that are cautious when it comes to binding themselves to international rules. As in the case of the EU and the US approaches, it can also be modified as required, for example by relaxing or strengthening rules on data localisation, by modifying the category of operators to which different types of obligations apply or by not requiring an outbound security assessment (or possibly by modifying what type of assessment is conducted in relation to outbound data). From the perspective of AfCFTA states, this would mean proposing not to include strong provisions on data flows (they could still, however, propose the inclusion of provisions on data protection, as the Chinese have done in some of their FTAs, for example their FTAs with Australia and South Korea).

It is of course possible for AfCFTA member states to adopt an approach that is completely unique or which combines different elements from the three dominant approaches sketched out above. Ultimately, however, each country

will have to assess the various aspects of the purported trade offs between economic integration and data protection. In doing so, they will have to ask to what extent the general privacy protection laws they have adopted (or may adopt in future) will be effective in the absence of transnational regulation. Simultaneously, they will have to examine what the potential economic benefits and drawbacks are of allowing data to flow freely in and out of their respective countries and to what extent measures can be taken to maximise gains, minimise losses while maintaining an appropriate level of data protection. Answering these questions will require a combination of empirical work on the economic implications of data protection and cross-border data flows and judgment calls that will ideally be based on a clear and principled strategy that is carefully and agilely monitored over time with a view to making appropriate adjustments where necessary.

---

[1] This essay is largely based on research undertaken for a policy brief produced as part of a Mandela Institute project titled ‘Africa’s Digital Economy: Protectionism, Development and Democracy’. The policy brief, titled ‘Data Protection in Kenya, Nigeria and South Africa in the 2020s and Beyond: Introducing a Mandela Institute Research Project’, is available .

View online: Symposium on the Economic Impacts of Data Localisation in Africa: Personal Data Protection and Economic Integration: Options for AfCFTA Negotiators

Provided by Afronomicslaw