Authors: Vincent Hofmann & Matthias Kettemann

Towards an African narrative on digital sovereignty

Data about people in Africa should remain in Africa and African states should have the autonomy to decide for themselves how to regulate their digital infrastructure and how to plan their digital futures. In brief: African states need to realize and own their digital sovereignty. But what does sovereignty mean? How can states achieve sovereignty?

The concept of digital sovereignty is one possible answer to the many challenges of digitalisation. But like many concepts that include legal and ethical aspects, it needs to be embedded in a socio-cultural context. Many of the widely used concepts on (parts of) digital sovereignty have their roots in the Global North. Therefore, using digital sovereignty as a guiding principle for digital development in African countries demands a reshaping of how we think of digital sovereignty. This is what the fellows of the research sprint on African digital sovereignty ventured out to do – with astonishing results.

Digital societies and the unequal distribution of power

Africa with its colonial history looks back onto a long period of an unequal distribution of power. Scrutinizing the current conditions of digitalisation, the threat of an unequal distribution of power looms large still today. Multilateral firms and foreign states control large parts of the digital infrastructure through their investments and African states have only few data centers which ensure local data ownership and control. Effective political oversight is not always guaranteed. This makes it hard for certain African countries to anticipate the influence of new digital technologies, which might bear the threat to undermine their ability to effectively steer the process of digitalisation.

This series of challenges can be explored through the lense of digital sovereignty. The notion of digital sovereignty is by no means a new one, but one that has gained prominence in digital economy debates due to the emergence of new geopolitical alliances and actors and the growing accumulation of power in large platform companies (Couture & Toupin, 2019).

Sovereignty as an elastic concept

Sovereignty is an elastic concept. As is the case with many ethical principles, interpretations and understandings of sovereignty differ widely. Different actors interpret the term for their own benefit in order to legitimize their exercise of power and control. When it comes to digital sovereignty, states invoke it to assert control over their 'cyber-jurisdictions' for purposes of digital development and national security. Groups, such as indigenous peoples and social movements, frame the term within a freedom-oriented narrative (Couture & Toupin, 2019). Nevertheless, there are concepts which include broadly accepted pieces of digital sovereignty: digital autonomy, the protection of grassroots innovation, data protection, and privacy. Key questions on perceiving a person or state as digitally sovereign are: Who owns the data? Who provides the services which people and states use, and who keeps the money

and knowledge generated by those services?

However, many of the accepted concepts on (parts of) digital sovereignty root in the Global North. Take data protection as an example. A robust data protection legal framework is strongly aligned with the concept of digital sovereignty, as it allows individuals to have control over their data (Vahisalu, 2019). Establishing an adequate level of data protection at the national level is therefore crucial. However, the data protection regimes originate from the European Union, the United States, and China. It is still unclear to which extent Global South countries can integrate these regimes into their national legal systems or whether the concept needs to be rethought. At the moment, many African countries lack a unified legal framework on data protection and - where relevant - rely on civil, criminal, and constitutional laws and individual rights of privacy (World Economic Forum, 2020). However, what might be a good solution for countries of the Global North can be of little use or even damaging for countries of the Global South. This has numerous reasons, including the special need for access to technology transfers, the lack of necessary digital skills (International Finance Corporation [IFC], 2019), and the need to improve infrastructure to facilitate the digital economy (Global Business Outlook, 2020).

African digital sovereignty

How can the concept of digital sovereignty be understood from an African perspective and how can it be achieved? What can be identified as another important step to achieve digital sovereignty in the African context, is keeping or regaining bigger parts of the value chain on digital processes. A homegrown economy through digitalisation, the growth of local technological start-ups, the integration of digital technologies into national sectors - such as finance, health and agriculture - the establishment of smart cities, and the boosting of internet connectivity through building homegrown internet infrastructure - including local data centers - are concrete steps towards this goal. However, this requires profound changes to the current situation.

Building and financing the necessary infrastructure

More scrutiny is needed, for example with regard to the current model of financing digital infrastructure, which sees large corporations come up with a “philanthropic” effort to provide internet connectivity to unconnected people in Africa. For instance, the Nigerian health data being hosted on platforms outside of Nigeria does not give adequate incentives for local digital development. To the contrary, it makes Nigeria’s health sector a super consumer of western solutions. Instead, local companies should be empowered to develop the capacity required to host country-generated content.

Increasing data ownership through regulation

While digital infrastructure deals with data storage, data ownership is about the generation and usage of data. Data ownership is influenced by technical infrastructures like data centers, but goes beyond this. The question is: Who generates the data and who enjoys the benefits of them? As many business models are highly data driven, this is a key factor towards successful digital services and the companies behind them. Currently, most of Africa’s data is collected and owned by foreign multilateral firms. To empower

local data ownership, African states should intensify efforts to reclaim infrastructural control by developing independent internet infrastructure to lessen dependencies (Fisher & Streinz, 2021), mandating data localisation and, most recently, carefully design the e-commerce protocol for the African Continental Free Trade Area to promote African interests (Kathure, 2021).

Fostering multinational cooperation

Fostering multinational cooperation has the power to boost the pursuit for digital sovereignty. For instance, cross-border data transfers, as part of data protection regulation, offer great potential for existing and upcoming businesses. Therefore, they should not only be generally allowed (although with exceptions for sensitive personal data), but should be supported by a harmonized framework of African data protection laws. In general, there should be more consolidated regulatory frameworks for African countries, spearheaded by the African Union, representing Africa as a single entity.

Implementing national AI strategies – a role model

The principles of African digital sovereignty could become binding rules in this and many other fields. For instance, the continuous growth of artificial intelligence (AI) offers great opportunities while leading to many challenges at the same time, not only for African countries. This development could be governed by national AI strategies which could be attributable to the principles of African digital sovereignty. As of 2021, only two African countries - Mauritius and Egypt - have such a strategy. With increasing caution towards western-developed models of digital policy and the desire and need for homegrown and socially responsive digital policy initiatives in Africa, Mauritius can serve as a model for African leaders looking to define Africa's tech policy trajectory and narrative in this new era. The nascent stage of Africa's digital economies and AI ecosystems should not preclude African governments from developing their own AI strategies and policy instruments for AI governance. Mauritius's national AI strategy is guided by the experiences of other nations, but not defined by them.

A long way to go

Digital sovereignty is a vague concept. But by digging deeper and exploring what digital sovereignty can mean for an African country, it can serve as a guiding principle with regard to concrete national regulation and transcontinental cooperation.

New scientific approaches to find the African narrative

This blog article is based on and uses parts of the publication of the Virtual Research Sprint: "Toward an African Narrative on Digital Sovereignty" hosted by the South African Research Chair for Industrial Development at the University of Johannesburg as part of The Ethics of Digitalisation project of the Network of Centers (NoC). Fellows from fourteen African countries and from a diverse range of

disciplinary backgrounds wrote a volume with twelve insightful pieces. Each of the pieces focuses on one particular field of digitalisation in the light of sovereignty from a truly African perspective.

Three key takeaways

1. Digital sovereignty is an elastic concept. It can be used in different ways by different actors to legitimize their goals and methods. Many of the accepted interpretations are based on narratives from the Global North. Striving for digital sovereignty in Africa therefore requires finding an African narrative on digital sovereignty.
2. In the African context, keeping or regaining bigger parts of the value chain on digital processes is key on the way towards digital sovereignty.
3. Regulators should boost digital sovereignty through (1) national but continent-wide harmonized data protection laws, (2) increasing data ownership through regulation as well as building and financing the necessary infrastructure, and (3) implementing national AI strategies like Mauritius did.

References

Couture, S. & Toupin S. (2019). What does the notion of "sovereignty" mean when referring to the digital? New Media and Society, 21(10): 2305-2322.

Fisher, A. & Streinz, T. (2021). Confronting data inequality. World Bank Development Report 2021 background paper, IILJ Working Paper 2021/1, NYU School of Law, Public Law Research Paper No. 21-22. Available from SSRN: https://ssrn.com/abstract=3825724 or http://dx.doi.org/10.2139/ssrn.3825724 (accessed 21.01.2022).

Global Business Outlook. (2020). Africa's efforts in digital transformation is vast. Available from: https://www.globalbusinessoutlook.com/africas-efforts-in-digital-transformation-is-vast/ (accessed 17.03.2022).

International Finance Corporation (IFC). (2019). Digital skills in Sub-Saharan-Africa: Spotlight on Ghana. Available from: https://www.ifc.org/wps/wcm/connect/ed6362b3-aa34-42ac-ae9f-c739904951b1/Digital+Skills_Final_WEB_5-7-19.pdf?MOD=AJPERES&CVID=mGkaj-s (accessed 17.03.2022).

Kathure, M. (2021, June 16). Africa's digital sovereignty: Elusive or a stark possibility through the AfCFTA? Afronomicslaw [Blog post]. Available from: https://www.afronomicslaw.org/category/analysis/africas-digital-sovereignty-elusive-or-stark-possibility-through-afcfta (accessed 21.01.2022).

Vahisalu, R. (2019, May 15). Digital sovereignty: The key to safeguarding Africa's booming digital

economy. Global Voice Group. Available from: https://www.globalvoicegroup.com/digital-sovereignty-the-key-to-safeguarding-africas-booming-digital-economy/ (accessed 21.01.2022).

Vatanparast, R. (2020). Data governance and the elasticity of sovereignty. Brooklyn Journal of International Law, 46(1):1-38.

World Economic Forum. (2020). A roadmap for cross-border data flows: Future-proofing readiness and cooperation in the new data economy. White Paper. Available from: http://www3.weforum.org/docs/WEF_A_Roadmap_for_Cross_Border_Data_Flows_2020.pdf (accessed 21.01.2022).