Centre for International
Governance Innovation

Policy Brief No. 185 — June 2024

Digital Sovereignty in Africa: Moving beyond Local Data Ownership

Folashadé Soulé

Key Points

- African states must be wary of conflating digital sovereignty with data localization, as this view overlooks the structural challenges that also need to be addressed to make data localization viable.
- Given the surge in data centres being built on the continent, there is a need for broader understanding of digital equity in terms of sharing the benefits of data, avoiding data colonialism and promoting African participation in data infrastructure development.
- Localizing sensitive government data, such as electoral information, is key to protecting digital sovereignty, necessitating enhanced local capacity in technology and data governance. African institutions can participate in driving this process by developing new financial models and capacity building in digital governance and cybersecurity.

Introduction

Digital sovereignty is an orientation and strategic position that aims to reaffirm the authority of state actors over cyberspace, including over the development of digital technology. As such, this vision requires recognition of the rights of individual countries to develop and use the policy instruments necessary to govern cyber activities within their legal territory (Musoni et al. 2023). A country's approach to digital sovereignty also depends on its economic and political interests, technological capabilities, national priorities and digital foreign policy. Internationally, there are several interpretations of the concept of digital sovereignty (ibid.) with variations from one continent to another.

In the European Union, the strategy has been to assert digital sovereignty by establishing global legal standards and promoting European technologies. The General Data Protection Regulation (GDPR)[1] is a notable example. It is part of the European strategy to impose strict standards on data governance and extend the European Union's authority over data processing, even beyond its borders. By setting these

1 See EC, *General Data Protection Regulation*, [2016] OJ, L 119/1, online: <www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/>.

About the Author

Folashadé Soulé is a CIGI senior fellow and senior research associate at the Global Economic Governance Programme, Blavatnik School of Government, University of Oxford. She is currently a visiting scholar at the University of Ghana. Her research areas focus on Africa-China relations, the study of agency in Africa's international relations and the politics of South-South cooperation. She is a principal investigator in Negotiating Africa's Digital Partnerships, a policy research project that examines Africa's relations with rising partners in the digital sector. As part of this project, she is leading a series of interviews and policy dialogues with African senior policy makers, ministers, and private and civic actors that aims to shed light on how African actors build, negotiate and manage strategic partnerships in the digital sector in a context of geopolitical rivalry. The views expressed in these interviews are reflected in this policy brief.

standards, the European Union encourages other regions to adopt laws similar to the GDPR.

The United States takes a laissez-faire approach, favouring unrestricted data flows, which benefits its technology companies, which control the largest share of the global market. However, through the CLOUD Act[2] (BSA 2021), the United States maintains its sovereignty by requiring US entities to disclose data upon request, for reasons of national security, regardless of its location.

China, meanwhile, maintains tight control over domestic and international operations. This approach results in surveillance-oriented data regulation and strict data transfer requirements. The Chinese government has privileged access to all data originating in China and requires companies to transfer critical information to state servers. Chinese companies are also required to provide access to their data for national security reasons when the state submits a request.

As part of the Negotiating Africa's Digital Partnerships policy research project,[3] hosted at the Blavatnik School of Government, University of Oxford, and supported by the Centre for International Governance Innovation, this policy brief reflects on perspectives gained from the interview series and aims to discuss approaches to digital sovereignty in Africa and its implications and challenges for data protection and digital transformation on the continent.

What Is Africa's Approach to Digital Sovereignty?

In Africa, a common misinterpretation is to draw a parallel between digital sovereignty and data localization. Some actors, particularly states but also regional financial institutions, believe that African governments can exercise their digital sovereignty by having greater control over data, infrastructure and all data-processing

2 See US, *Clarifying Lawful Overseas Use of Data Act*, Pub L No 115-141, 115 Cong (2018) (enacted), online: *Congress.gov* <www.congress.gov/bill/115th-congress/house-bill/4943>.

3 See www.geg.ox.ac.uk/negotiating-africas-digital-partnerships-interview-series.

activities taking place on their territory, if digital infrastructure and data centres are located on the African continent and owned by African entities (for example, see African Development Bank Group 2024). The proponents of this concept, which include some African governments, seek on the one hand to emphasize the nation-state as the main vector of cyberspace governance, while on the other hand taking advantage of companies and private investment to promote digital development (Soulé 2023).

These economic sovereignty initiatives include significant investments to create new national data centres (major projects have been launched in this direction in Benin, Congo, Côte d'Ivoire, the Senegalese city of Diamniadio, Togo and other parts of Africa) and internet exchange points. Although data localization is seen as a means of ensuring data sovereignty, it remains difficult to achieve, mainly due to the financial resources and technical capabilities required to deploy the data centres that would be needed to meet this requirement. A Nigerian media outlet reported in 2021 that 70 percent of Nigerian government agencies hosted their data on cloud storage based overseas (Guardian Nigeria 2021). Therefore, several African states place the construction of data centres at the heart of their ambition for digital sovereignty, often in cooperation with international financial institutions such as the World Bank or with the help of Chinese loans.

The Surge in Data Centres in Africa: A New Data Capitalism?

In response to the acceleration of digitalization, several African countries have built or are building data centres with the help of foreign investments and companies. Many African governments are also working to force companies to store their data locally, although this tactic does not necessarily lead to digital development or better-protected data, as these countries also struggle to provide reliable electricity supplies and high-speed connectivity (Global Economic Governance Programme 2023a).

The surge in data centre construction in Africa (estimated at around 700 new facilities over the next decade), reflecting the continent's digital dependence, represents what some analysts are calling a phase of "data capitalism" (Global Economic Governance Programme 2023d). In the European Union, data is regulated and protected under the GDPR, but in Africa, data protection is far less consistent, and governed by the African Union (AU) Convention on Cyber Security and Personal Data Protection (Malabo Convention), the continent's comprehensive regulation on cybersecurity, which only a few countries have finally ratified (ibid.). The lack of comprehensive regional data protection laws further complicates this issue.

Many African nations lack robust data protection legislation, which raises concerns about whether these emerging data centres can be effectively regulated. This is especially concerning as several African countries are embarking on national digital ID projects that require the collection, storage and processing of sensitive data in data centres. Despite some countries, such as Ghana, making progress with digital ID systems, there is a general lack of widespread, systematic data collection across the continent — thousands of people in Africa still have no civil registration records (for example, birth certificates), and in places where these exist, they are largely not yet digitalized (ibid.).

An important consideration is the question of who the primary beneficiaries of these data centres are. Africa must approach discussions on data centrality cautiously, addressing digital inequalities to ensure reciprocal and equitable access, use and benefits from this data. This process will be helped by an increase in African-owned or -driven data centre construction and operations initiatives. However, despite projections of growth in the number of data centres on the continent, power availability and connectivity issues make this digital infrastructure a daunting venture for all but the largest investors. This disparity raises questions about true digital sovereignty and local data ownership in Africa. There appears to be a misunderstanding of digital sovereignty in the African context. For instance, African leaders might readily share comprehensive national data with international corporations such as Google, which may fund data centres, without fully considering the implications for data sovereignty and security. This practice extends to areas such as election infrastructure, often managed

by foreign companies, with data domiciled outside Africa. The critical issue, then, is whether these data centres are being constructed to genuinely build capacity within Africa or to serve external interests, a situation that scholars have argued can be a form of "data colonialism" (Coleman 2019). Until there is a broader understanding and discussion about what digital equality means for Africa, it will be challenging to achieve parity in the global digital landscape. This conversation is essential to ensure that Africa's development in the digital age is equitable and beneficial to its people.

The Risks for African Governments Relying on the Chinese Model of Data Protection

Several African countries have also introduced data governance frameworks that resemble those in China. In 2021, Senegal was notably the first African country to replicate the Chinese data governance model, which requires all servers to be located within the country's borders (Olander 2021). The state transferred government data and digital platforms that were stored on servers abroad to a data centre built by Huawei in Senegal. This data centre was financed by a Chinese loan. According to the director of Sénégal Numérique, the government digital development agency, "this state-of-the-art datacentre allows Senegal to better control its destiny and to definitively resolve the issue of its digital sovereignty" (Global Economic Governance Programme 2023b).

This arrangement, however, poses several problems. The danger of relying on Chinese surveillance technologies to ensure the digital sovereignty of African countries has been somewhat obscured by China's advocacy of data sovereignty at various global digital technology standards bodies (Global Economic Governance Programme 2023f). Investigations have revealed that confidential data from the headquarters of the African Union built by China was diverted every night from Addis Ababa, Ethiopia, to Shanghai, China, and therefore accessible to the Chinese government (Kadiri and Tilouine 2018). China is far from the only power to use the internet for espionage, as US intelligence services have accessed the data of millions of citizens around the world, including in Africa (BBC News 2014; *Le Monde* 2016).

Furthermore, while this push for digital sovereignty and its emphasis on data localization seemingly empowers local actors, it also raises questions about digital rights and the capacity of civil society to promote these rights and combat abuses by local governments and excesses of private companies (Global Economic Governance Programme 2023e).

Thus, while data centres and related infrastructure can improve the quality of service delivery to end users, it remains to be proven whether this contributes significantly to digital sovereignty. Many digital services, including those managed by governments, are still hosted on servers outside the continent. As long as indigenous technological capabilities remain underdeveloped, achieving data sovereignty will remain an elusive goal (Global Economic Governance Programme 2023f).

According to Motolani Peltola, Tampere University, "The surge in efforts by African governments to bolster digital sovereignty and local data ownership encompasses economic, social and political dimensions. The rationale behind the adoption of data localization requirements includes considerations for cybersecurity, data protection and privacy of citizens, economic development, law enforcement, national security and, controversially, government censorship and surveillance. While these motivations hold true for African countries, the predominant reasons often revolve around data protection and economic development. For instance, Nigeria's data localization policy is justified by the aspiration to rectify the negative trade balance in the information and communications technology sector and foster a digital economy for the benefit of its citizens. Similarly, South Africa views data and associated digital infrastructure as strategic national resources" (Global Economic Governance Programme 2023c).

The Dual Challenge of Data Storage and Data Protection

Peltola explains, "Through the implementation of data localization regulations, certain African governments aim to mitigate the risk of data colonization, reinforce digital sovereignty and ensure local economies reap the benefits. The prevalence of foreign technology firms in Africa, with their access to valuable user data, exposes African governments and citizens to data and national security vulnerabilities. Local hosting of data is envisioned as a means for African governments to maintain control over critical data and data infrastructure, such as data centres, with some countries designating them as critical information infrastructure to be protected as strategic national assets yielding socio-economic benefits" (ibid.).

Complete data localization is an ambitious and perhaps unattainable goal. Nevertheless, there is a growing trend toward internet fragmentation and data localization, as seen in countries such as Senegal. This country has been active in cybersecurity and vocal about its digital sovereignty, as evidenced by its ratification of the Malabo and Budapest Conventions (the latter of which is also focused on cybersecurity). Senegal's move toward data onshoring, with support from China, raises important questions. The 2019 incident at the African Union, where servers at its Chinese-built headquarters were allegedly secretly transmitting data to China, highlights the potential disconnect between the stated goals of such initiatives and their actual outcomes (Global Economic Governance Programme 2023d).

The practicality of full data localization in Africa is also questionable. Technology companies and infrastructure are predominantly foreign, and the applications of data often have international dimensions. Moreover, cybersecurity requires a degree of international cooperation, meaning that external powers may still have access to data despite localization efforts. This reality underscores the importance of examining the dynamics of international conventions and treaties from a unified African perspective. While the ambition of countries such as Senegal in localizing government data is laudable, it is unclear whether this approach will be feasible across Africa. A more harmonized approach to data protection would be more suitable, in which African countries collectively define their priorities and develop a deeper understanding of data governance (ibid.).

The effectiveness of strategies for African governments to achieve consensus and action in the digital sphere is influenced by a variety of factors, some of which are human-made, while others are inherent to the region's realities, such as political instability and conflict. These factors often shift the priority away from digital goals. For instance, the African Union experienced a significant cyberattack in 2024, yet the response was unclear, reflecting the overarching issue of prioritizing physical conflicts over digital threats. The African Union, unlike the European Union, does not have the same regional influence and is relegated to observer status in cybercrime negotiations. This limitation hinders the African Union from speaking for or holding its member states accountable in digital matters (ibid.).

The individualized approach to governance in African countries impacts cyber governance. While the African Union has started pursuing a unified African position on cybersecurity, a mere policy document does not necessarily equate to consensus, as evidenced by the limited impact of the Malabo Convention.

Various Responses to the African Discourse on Local Data Ownership

According to Peltola, "The responses of foreign state actors, such as China, European countries and the United States, to the discourse surrounding data localization in Africa, can be seen as reflective of their domestic approaches to digital sovereignty, data protection and regulation. While the European Union and Africa share concerns regarding the dominance of foreign technology firms and their use of citizen data, there are disparities in their approaches to digital sovereignty. The European Union champions a liberal stance on digital sovereignty, emphasizing individual control over data rather than government or private sector

oversight, contrasting with African countries' tendencies to exhibit elements of both state-centric and liberal models in their approaches to data sovereignty to varying degrees" (Global Economic Governance Programme 2023c).

"Conversely," Peltola adds, "both the European Union and the United States have expressed concerns about the discourse on local data ownership in Africa, particularly with respect to the implications of increasing governmental control over data for civil liberties and the potential misuse of data by authoritarian governments. Also, there are concerns regarding the national security risks posed by digital infrastructure provided by state-led Chinese companies. Additionally, questions surround the competitiveness of European tech companies amid increasing data localization regulations in a sector dominated by Chinese and American technology firms. The complexity of the landscape is further compounded by the European Union's efforts to strengthen its position in the global data value chain, to promote competitiveness and to negotiate agreements with African countries on digital-related clauses" (ibid.).

The United States, adopting a more liberal approach to data sovereignty, has historically abstained from imposing federal or comprehensive data localization requirements. The dominance of US technology companies around the world and the country's historical advocacy for open cross-border data flows reflect a liberal regime on data localization with limited restrictions. While debates on data localization continue, there is no formal consensus among US policy makers on domestic mandates, and foreign policy responses have yet to materialize. Still, the United States is primarily concerned about the economic impact on American businesses of restricted cross-border data flows, and fears of an authoritarian approach to data governance stemming from China's growing dominance in the provision of digital infrastructure in Africa, which is driving the trend toward increased data localization on the continent. For example, the Office of the US Trade Representative has expressed concerns about data localization measures in Nigeria and Kenya, which it considers discriminatory against foreign companies (which store and process data globally) and potentially harmful to the development of the digital economy.[4]

According to Peltola, "China, adopting a state-centric view of digital sovereignty, centralizes the role of the state in data governance and citizen data control. Enforcing a strict data localization approach and mandating data to be hosted within the state of its production, China has propelled the growth of its domestic firms at the expense of foreign competitors. In Africa, China's active involvement in financing digital infrastructures, including data centres, and its technology companies' collaboration with governments in designing national digital economy strategies, exemplifies its commitment to shaping the digital landscape in alignment with its Digital Silk Road aims" (ibid.).

"A common thread in the response of foreign actors, namely, the United States, China and the European Union, is a concerted effort to bolster the competitiveness of their technology firms globally, particularly in Africa's technology sector, which still holds substantial investment opportunities. Despite the variations in their domestic stances on data localization, these actors — the United States (Karombo 2020), China (State Council, People's Republic of China 2023) and the European Union[5] — demonstrate an interest in capitalizing on the investment opportunities facilitated by the growing trend of data localization in Africa" (ibid.).

Recommendations

Localizing government data, particularly sensitive information such as electoral data, within the country is a crucial step toward safeguarding digital sovereignty. African countries need to build their capacity in technology and data governance to make this ambition realistic. While the aspiration to localize data is not far-fetched and is indeed being pursued by other countries, the transition to such a model in Africa needs careful consideration, balancing ambition with the realities of technological dependence and international cooperation.

Furthermore, the African Union needs to prioritize funding and capacity building in digital governance and cybersecurity. Currently, many

4 See https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2019/march/fact-sheet-2019-national-trade-estimate.

5 See https://futurium.ec.europa.eu/en/Digital4Development/discussion/eu-au-data-flagship.

African countries rely on capacity building provided by external states, leading to a lack of a harmonized approach. This situation is compounded by donor superiority, where external countries often dictate Africa's digital priorities.

Moreover, it will be crucial for more African countries to develop and implement robust data protection and privacy regulations. These policy processes should consider continental data governance frameworks such as the African Union's Data Policy Framework, which underscores the importance of building stakeholder engagement at all levels to ensure data is used to further public interests, with a specific focus on cloud computing, big data services and platformization. This approach will be essential to foster system efficiency, decision-making improvements, and the facilitation of an African model of cross-border data transfers that promotes rather than hinders intracontinental trade (Gehl Sampath and Tregenna 2022).

Regional economic communities such as the Economic Community of West African States (ECOWAS) play a significant role, but they face subregional governance challenges. Even with directives such as the ECOWAS Regional Cybersecurity and Cybercrime Strategy, inconsistencies such as internet shutdowns within member states reveal gaps in implementation and adherence.

Another strategy could involve African "champion" countries, such as Egypt, Ghana, Mauritius, Morocco and Rwanda, that have shown leadership on specific digital governance issues, leading and guiding others toward specific collective goals. This approach has already shown promise on the continent, for example, with progress on the Malabo Convention. In March 2022, Togo successfully rallied select African heads of state to adopt the Lomé Declaration on cybersecurity and the fight against cybercrime, through which signatories committed to sign and ratify the Malabo Convention. The convention finally went into force in June 2023 after the minimum required 15 AU member states ratified it. The next steps may involve using this momentum as a platform to steer the development of a harmonized approach and adapt the convention to better suit local or regional needs.

The African Union's Digital Transformation Strategy, if implemented transparently and accountably, could provide a robust framework for the continent's digital evolution. Ensuring transparency and accountability in implementing this strategy would help define Africa's digital governance landscape more effectively.

Author's Note

This policy brief was updated in September 2024.

Works Cited

African Development Bank Group. 2024. "Congo: New data centre funded by African Development Bank will cement national and subregional digital sovereignty." News and events, May 17. www.afdb.org/en/news-and-events/congo-new-data-centre-funded-african-development-bank-will-cement-national-and-subregional-digital-sovereignty-70847.

BBC News. 2014. "Edward Snowden: Leaks that exposed US spy programme." BBC News, January 17. www.bbc.com/news/world-us-canada-23123964.

BSA. 2021. "What Is the CLOUD Act?" www.bsa.org/files/policy-filings/09012021whatiscloudact.pdf.

Coleman, Danielle. 2019. "Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws." *Michigan Journal of Race and Law* 24 (2): 417–39. https://doi.org/10.36643/mjrl.24.2.digital.

Gehl Sampath, Padmashree and Fiona Tregenna, eds. 2022. *Digital Sovereignty: African Perspectives.* Johannesburg, South Africa: DSI/NRF South African Research Chair in Industrial Development. https://doi.org/10.5281/ZENODO.5851685.

Global Economic Governance Programme. 2023a. "Bulelani Jili: 'African policymakers should see digital development, data flows, and data governance as mutually reinforcing.'" Negotiating Africa's Digital Partnerships interview. www.geg.ox.ac.uk/content/bulelani-jili-african-policymakers-should-see-digital-development-data-flows-and-data.

———. 2023b. "Cheikh Bakhoum, Sénégal Numérique: 'Geopolitical rivalries in the digital sector could foster positive competition for Africa.'" Negotiating Africa's Digital Partnerships interview. www.geg.ox.ac.uk/content/cheikh-bakhoum-senegal-numerique-geopolitical-rivalries-digital-sector-could-foster.

———. 2023c. "Motolani Peltola: 'The pursuit of digital sovereignty and local data ownership has implications for local capacity development.'" Negotiating Africa's Digital Partnerships interview. www.geg.ox.ac.uk/content/motolani-peltola-pursuit-digital-sovereignty-and-local-data-ownership-has-implications.

———. 2023d. "Nnenna Ifeanyi-Ajufo: 'The current state of cybersecurity in Africa is the tendency towards a cyber-militarisation approach.'" Negotiating Africa's Digital Partnerships interview. www.geg.ox.ac.uk/content/nnenna-ifeanyi-ajufo-current-state-cybersecurity-africa-tendency-towards-cyber.

———. 2023e. "Teki Akuetteh, Africa Digital Rights Hub: 'Civil society organisations have the power to hold governments accountable on digital rights enforcement.'" Negotiating Africa's Digital Partnerships interview. www.geg.ox.ac.uk/content/teki-akuetteh-africa-digital-rights-hub-civil-society-organisations-have-power-hold.

———. 2023f. "Tin Hinane El Kadi: 'Collective bargaining would help maximise gains from negotiations with leading tech firms.'" Negotiating Africa's Digital Partnerships interview. www.geg.ox.ac.uk/content/tin-hinane-el-kadi-collective-bargaining-would-help-maximise-gains-negotiations-leading.

Guardian Nigeria. 2021. "70% of govt agencies host data abroad despite $220m local infrastructure." *The Guardian* (Nigeria), June 4. https://guardian.ng/technology/70-of-govt-agencies-host-data-abroad-despite-220m-local-infrastructure/.

Kadiri, Ghalia and Joan Tilouine. 2018. "A Addis-Abeba, le siège de l'Union africaine espionné par Pékin." *Le Monde*, January 26. www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html.

Karombo, Tawanda. 2020. "The US development corp is betting $300 million on Africa's rising demand for data storage." *Quartz*, December 11. https://qz.com/africa/1945156/us-dfc-bets-300m-on-africas-demand-for-data-storage-centers.

Le Monde. 2016. "Révélation Snowden : l'Afrique et les télécoms sous surveillance massive." *Le Monde*, December 8. www.lemonde.fr/pixels/article/2016/12/08/revelations-snowden-les-elites-africaines-et-les-techniciens-des-telecommunications-surveilles-par-les-americains-et-les-britanniques_5045480_4408996.html.

Musoni, Melody, Poorva Karkare, Chloe Teevan and Ennatu Domingo. 2023. "Global approaches to digital sovereignty: Competing definitions and contrasting policy." ECDPM Discussion Paper No. 344. May. https://ecdpm.org/work/global-approaches-digital-sovereignty-competing-definitions-and-contrasting-policy.

Olander, Eric. 2021. "The Powerful Symbolism of The Huawei-Built Data Center Deal in Senegal." China Global South Project, June 24. https://chinaglobalsouth.com/analysis/the-powerful-symbolism-of-the-huawei-data-center-deal-in-senegal/.

Soulé, Folashadé. 2023. *Navigating Africa's Digital Partnerships in a Context of Global Rivalry*. CIGI Policy Brief No. 180. Waterloo, ON: CIGI. www.cigionline.org/publications/navigating-africas-digital-partnerships-in-a-context-of-global-rivalry/.

State Council, People's Republic of China. 2023. "China to strengthen digital cooperation with African countries." October 20. https://english.www.gov.cn/news/202310/20/content_WS653213d0c6d0868f4e8e0799.html.

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

Managing Director of Digital Economy Robert Fay (until February 2024)
Director, Program Management Dianna English
Program Manager Jenny Thiel
Publications Editor Susan Bubak
Graphic Designer Abhilasha Dewan

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org