NATIONAL DIGITAL SOVEREIGNTY AND ITS SOCIO-ECONOMIC IMPACT ON AFRICAN COUNTRIES

Emmanuel Chinanu Uwazie
Department of Computer Sciene
Catholic University of Cameroon
uwazie.e@catuc.org

John Ojima Mamman
Department of Mathematics
Federal college of Education
Abeokuta, Ogun, Nigeria
mammanojima@gmail.com

Joel B. Abah
Department of Computer Science
Chinanu Technology Institute
Abuja, Nigeria
abahjoel@yahoo.com

Tahir Abdulhakim
Department of Computer Science
Nasarawa State University Keffi
Nasarawa, Nigeria
abdullahitahir@nsuk.edu.ng

Abstract

National digital sovereignty is closely related to data protection regulation. National digital sovereignty refers to a country's ability to control and govern its digital infrastructure, data, and online activities within its borders. Data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union, are essential components of national digital sovereignty. These regulations ensure data privacy and security for citizens, establish guidelines for data processing, storage, and transfer. They also provide oversight mechanisms for data handling practices and impose penalties for non-compliance. However, there are some drawbacks associated with Data localization laws in Africa. Therefore, they require careful consideration of these socio-economic impacts to maximize benefits while minimizing potential drawbacks. This paper aims to highlight the merits and demerits of data localization laws in Africa.

Keywords: *Sovereignty, Data, Protection, Africa, Regulation*

How to Cite:
Uwazie, E. C., Okonkwo, N. U., Ezeaku, F.N. (2026). The Effect of Artificial Intelligence on Education: Oppurtunities, Applications and Challenges. *Central African Journal of Science and Technology*, 1(1), 74–79

INTRODUTION

National digital sovereignty and data protection regulation are interconnected in several ways. Firstly, by data localization whereby countries may require data to be stored and processed within their borders to maintain control and jurisdiction. Then by data transfer in which regulations govern the transfer of data across borders, ensuring that data is protected and compliant with local laws. Also by jurisdiction wherein data protection regulations assert a country's jurisdiction over data processing and handling. And by sovereignty whereby national digital sovereignty ensures that countries have the authority to enforce data protection laws and regulations. Other aspects of national digital sovereignty related to data protection regulation are: data ownership, data governance, data security, cross-border data transfer, regulatory oversight and enforcement mechanisms. These regulations are crucial for maintaining national digital sovereignty and ensuring data protection in Africa. Key stakeholders of data protection regulation and sovereignty include governments, private sector, civil society, international organizations and local communities. National digital sovereignty and data protection regulation are intertwined concepts that aim to protect citizens' data privacy and security, assert national control over digital infrastructure and data and ensure compliance with local laws and regulations. Some examples of data protection regulations related to national digital sovereignty in African nations include Nigeria Data Protection Regulation (NDPR, 2019), which establishes guidelines for data processing, storage, and transfer. South Africa's Protection of Personal Information Act (POPIA, 2013) which regulates data processing, storage, and transfer. Egypt's

Personal Data Protection Law (Law No. 151, 2020) that governs data processing, storage, and transfer. Kenya's Data Protection Act (DPA, 2019), establishing guidelines for data processing, storage, and transfer. Morocco's Data Protection Law (Law No. 09-08, 2009), regulating data processing, storage, and transfer. Ghana's Data Protection Act (DPA, 2012) which establishes guidelines for data processing, storage, and transfer. Rwanda's Law on Protection of Personal Data (Law No. 58/2018) that regulates data processing, storage, and transfer. Tunisia's Organic Law on the Protection of Personal Data (Law No. 63-2019), establishing guidelines for data processing, storage, and transfer. Algeria's Law on the Protection of Personal Data (Law No. 18-07, 2018) that regulates data processing, storage, and transfer. Mauritius' Data Protection Act (DPA, 2017), establishing guidelines for data processing, storage, and transfer. These regulations demonstrate African nations' efforts to: protect citizens' data privacy and security; assert national control over digital infrastructure and data; ensure compliance with local laws and regulations; foster trust in the digital economy and align with international data protection standards. These countries in Africa strive to balance national digital sovereignty with global data flows, international cooperation, and economic interests. However, data localization laws in African nations can have significant socio-economic impacts which are both positive and negative. Economic sectors affected include telecommunications, finance and banking, e-commerce, healthcare, education and government services. Therefore, national digital sovereignty in African nations requires careful consideration of these socio-economic impacts to maximize benefits while minimizing potential drawbacks.

CASE STUDIES

The issues surrounding digital sovereignty and independence also highlight the challenges African nations have in securing foreign aid, the most significant of which being the opposing parties' interests in trade agreements. Significant contributions to the investment environment in Africa's digital sector have come from both Eastern and Western partners. For instance, China's Digital Silk Road initiative emphasizes the Eastern perspective on Africa's digital growth and calls for large investments in broadband networks and smart cities, among other digital infrastructure projects. One initiative that stands out under this program is the collaboration between Huawei and other African nations to deploy 5G networks. These networks are built in China and offer cuttingedge digital services like internet connectivity and e-commerce. [1].

In an attempt to regain control over their citizens' data, African governments have begun onshoring it by investing in brand-new national data centres, such as those in Benin and Togo. By enabling governments to handle data locally, these centres would stop exploitation. Moreover, these centres are usually not supported autonomously, but rather through cooperative political organisations (such as the World Bank and the International Monetary Fund, among others); when funding is contingent on a single donor, African nations have ensured that oversight and infrastructure are managed locally by their own citizens.[2].

IMPACT ANALYSIS

Following historic colonial patterns of resource exploitation that benefit the local populace only minimally, these corporations often collect, process, and sell African data back to African consumers [3]. The commodification of data has important economic repercussions because large multinational firms derive most of their profits from the value extracted from raw data, whereas data analysis and utilisation do not assist African economies. A significant contributing element to this is the lack of standard privacy and data protection legislation in Africa, such as the 2014 African Union Convention on Cybersecurity and Personal Data Protection law, which was signed by 14 nations but ratified by just 8 as of 2020.

The implementation of national digital sovereignty and data protection regulations has numerous positive impacts, including job creation, economic growth, improved data security, and asserting national sovereignty. Data localization requirements can stimulate local economies by increasing demand for domestic data centers, generating jobs in construction, maintenance, and management. Additionally, national digital sovereignty fosters economic growth through investments in digital infrastructure and services. Local data storage also enhances data protection and security by reducing reliance on foreign data centers. Furthermore, data localization asserts national control over digital infrastructure and data, while promoting local content and cultural diversity, thereby preserving cultural heritage. Overall, these regulations empower nations to safeguard their digital interests, foster economic development, and protect their citizens' data.

The implementation of national digital sovereignty and data protection regulations can have several adverse consequences, including internet fragmentation, reduced competition, technical challenges, increased costs, and facilitated censorship and surveillance. By requiring data localization, nations risk undermining global interoperability and creating a fragmented internet. This can also limit foreign investment and competition, stifling innovation and potentially harming local businesses. Moreover, local data centers may struggle to match international standards for security, scalability, and reliability, while the costs of building and maintaining these centers can be prohibitively expensive, leading to higher prices for consumers. Furthermore, national digital sovereignty can provide governments with greater control over online content and user data, potentially enabling censorship and surveillance, thereby threatening individual privacy and freedom of expression.

The implementation of national digital sovereignty and data protection regulations can have significant social implications, potentially exacerbating existing digital divides, limiting freedom of expression, and raising privacy concerns. If local infrastructure is underdeveloped, data localization requirements can widen the gap between digitally connected and disconnected communities. Moreover, overly restrictive laws can restrict access to information and stifle free speech, undermining democratic values. Additionally, local data storage can increase vulnerability to government surveillance and data misuse, eroding trust in digital services and compromising individuals' right to privacy. These consequences can disproportionately affect marginalized groups, amplifying existing social inequalities and highlighting the need for balanced regulations that prioritize digital inclusion, freedom, and protection.

CHALLENGES AND OPPORTUNITIES

To address the issues brought on by the commodification of data, robust frameworks for data governance are required at the national and continental levels.

As African markets became more accessible to international technology commerce, foreign corporations began to progressively dominate infrastructure, software, and services [4]. In addition to being technological, this reliance includes digital commerce and data control, which put national sovereignty at risk by consolidating power in the hands of a small number of foreign governments and multinational enterprises.

Globalisation had a critical role in promoting innovation in African industries such as banking and infrastructure, and it also contributed to the creation of the digital gap - an additional layer of inequality between African countries and foreign powers. At the price of political or economic enslavement, these forces have continuously utilised their clout to promote progress [2].

The competing agendas of their respective agreeing partners are demonstrated by China's Digital Silk Road initiative and the European Union's D4D strategy. Due to the political complexities between these partners, African countries may be left unsure of what to prioritise, which could lead to an inconsistent digital system. [5].

This should not take away from the significant opportunities for advancing technical and economic development throughout the continent.

Africa must keep moving forward in a number of areas, such as enhancing digital infrastructure, fostering innovation, and establishing robust regulatory frameworks, if it is to be able to provide job opportunities [5]. To gain popular support, African governments have begun utilising digital tools—which are under the authority of foreign entities—for citizen engagement, monitoring, and service delivery. This is due to the fact that the availability of digital technology to the general public is now crucial for both industrial and economic development. [6].

In order to preserve national data sovereignty, provide just recompense for their data resources, and encourage the growth of regional data analytics enterprises, African countries must create laws and policies.

According to the African Union Commission (2020), this strategy is essential for turning data into a tool for sustainable development rather than a resource that is used by outside parties [7].

RECOMMENDATION

To effectively implement national digital sovereignty and data protection regulations, policymakers should strike a balance between data localization and global cooperation, adhering to international standards while promoting local infrastructure and skills development. Regulations should be proportional, flexible, and harmonized across regions to facilitate cooperation and avoid fragmentation. Investing in local digital infrastructure and skills development will enhance capacity and competitiveness. Furthermore, fostering regional cooperation and harmonization will ensure consistency and efficiency. Finally, ongoing monitoring and evaluation of socio-economic impacts are crucial to assess the effectiveness and adjust policies accordingly, ultimately ensuring that national digital sovereignty and data protection regulations promote digital inclusion, innovation, and economic growth while safeguarding individual rights.

REFERENCES

[1] Huawei. 2023. “New Opportunities of 5G FWA in Africa, Addressing the Gap in Last-mile Fixed Broadband Connectivity.” Press release, November 16. www.huawei.com/en/news/2023/11/africa5gsummit.

[2] 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/navigatingafricas-digital-partnerships-in-a-context-of-global-rivalry/.

[3] Couldry, Nick and Ulises A. Mejias. 2019. The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism. Stanford, CA: Stanford University Press.

[4] Mann, Laura. 2018. “Left to Other Peoples’ Devices? A Political Economy Perspective on the Big Data Revolution in Development.” Development and Change 49 (1): 3–36. https://doi.org/10.1111/dech.12347.

[5] Tyler Stevenson Navigating digital Neocolonialism in Africa "Centre for International Governance Innovation and CIGI" 2024

[6] Jain, Nick. 2024. “What is Digital Transformation in Government? Definition, Roles, Benefits, Challenges and Trends.” IdeaScale (blog), February 23. https://ideascale.com/blog/what-is-digital-transformation-in-government/.

[7] African Union Commission. 2020. The Digital Transformation Strategy for Africa (2020–2030). https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf.