Centre for International Governance Innovation

Digital Policy Hub

Digital Policy Hub – Working Paper

Harmonization of Data Governance Frameworks in Africa

Badriyya Yusuf

Summer 2024 cohort

About the Hub

The Digital Policy Hub at CIGI is a collaborative space for emerging scholars and innovative thinkers from the social, natural and applied sciences. It provides opportunities for undergraduate and graduate students and post-doctoral and visiting fellows to share and develop research on the rapid evolution and governance of transformative technologies. The Hub is founded on transdisciplinary approaches that seek to increase understanding of the socio-economic and technological impacts of digitalization and improve the quality and relevance of related research. Core research areas include data, economy and society; artificial intelligence; outer space; digitalization, security and democracy; and the environment and natural resources.

The Digital Policy Hub working papers are the product of research related to the Hub's identified themes prepared by participants during their fellowship.

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.

Partners

Thank you to Mitacs for its partnership and support of Digital Policy Hub fellows through the Accelerate program. We would also like to acknowledge the many universities, governments and private sector partners for their involvement allowing CIGI to offer this holistic research environment.

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

Key Points

- Data access and exchange offers benefits but also brings to the fore concerns about privacy rights, ethical implications and the effectiveness of existing regulatory frameworks.
- Regional approaches to data governance help enhance interoperability and harmonization of national data regulations.
- Recognizing diversity in levels of technological development, political economic analysis and context-specificity consideration all play a role in African data governance.

Introduction

Defined as a set of policies, processes and roles that determine how an entity manages and controls its data (CSM Tech 2024; Ladley 2019), effective data governance has become a strategic necessity for governments around the world. Concerns about privacy rights, ethical implications and the effectiveness of existing regulatory frameworks further complicate cross-border data sharing and access. As the global economy becomes increasingly data driven, developing countries with weak or absent data protection frameworks are projected to encounter more obstacles participating and competing in it (Aaronson 2018).

Recognizing the importance of data privacy and protection, at least 36 out of 55 African states have some form of data protection regulation or national data plan as of 2023.[1] While some states have strong legislation, others are still in the early stages of development or amending previous regulations. For example, Nigeria, which had previously relied on its Nigeria Data Protection Regulation (2019), only recently signed into law the Nigeria Data Protection Act (2023) after much criticism about loopholes and the need for more comprehensive and enforceable legislation from local stakeholders and other African states in the region (KPMG 2023).

Differences in sociopolitical context also result in varied levels of regulation enforcement, compliance and public awareness of privacy rights. This poses challenges to the growth of pan-African digital services, interoperability and harmonization of cross-border policies (Yusuf 2024). Given the different digital development levels and maturity of data regulations in Africa, there is a growing need for harmonized data governance frameworks across the continent. Regional approaches have been advocated as a way forward in coordinating data governance (Balogun and Adeniran 2024; Internet & Jurisdiction Policy Network 2022). Regional frameworks have the potential to facilitate cross-border data flows essential for the African Free Trade Area (African Union 2023), which is expected to be the world's largest, covering a market of more than 1.3 billion people across 55 countries with a combined GDP of more than US$3.4 trillion (World Bank 2020). Regional frameworks also pave the way for achieving the vision of an African single data market and attracting international investors and technology

1 See https://dataprotection.africa.

companies, which necessitates the integration of markets, implementation of uniform online payment services, standardization of taxation and facilitation of cross-border trade (Thaldar 2023).

As such, the effectiveness of existing instruments of data governance is critical in laying the foundations for the regulation of emerging technologies. This working paper contributes to a series of Digital Policy Hub working papers focused on addressing the question of how to develop sustainable data frameworks in Africa. The series explores the increasingly complex policy challenges and opportunities for developing data policy frameworks and regulatory approaches for digital transformation in the Global South. The first paper in the series provided an environmental scan of the African digital landscape and the implications for cross-border data flows (Yusuf 2024). This second paper advances the discussion by exploring the extent to which the disparate data governance models in the region accommodate the continental strategies. It proceeds as follows: First, an overview is provided of the potential of — and gaps in — promoting safe and ethically sound data flows of selected existing continental instruments. Next, the implementation challenges of existing frameworks are identified, including case studies to demonstrate the impact of variances in national data frameworks. The third section provides recommendations based on the study's findings.

Methods

To deepen our understanding of the challenges, opportunities and outcomes of data governance frameworks in Africa, this research uses qualitative methods. A desk review of publicly accessible government, intergovernmental and non-governmental organization reports, as well as expert interviews, is used to help delve into explanations that may be insufficiently nuanced or contextualized in quantitative research. The paper also uses a case-study approach to help illustrate how varied sociopolitical contexts and levels of technological advancement in African countries impact the development of sustainable data frameworks.

Overview

Despite variations in national data regulations, Beverley Townsend (2021) identifies several fundamental principles of personal data protection that are common across many countries. These are:

- **Fair and lawful processing:** Data must be handled in a way that is both legal and ethical.
- **Purpose limitation:** Data should only be used for specific predetermined purposes.
- **Data minimization:** Collection should be limited to what is necessary, relevant and not excessive for the intended purpose.
- **Data subject access and control:** Individuals should have the right to access their data and exercise control over its use.

- **Security and disposal:** Data must be kept secure and destroyed once it has served its purpose.
- **Enhanced protection for sensitive data:** Certain types of personal information require stricter safeguards.

In addition, the harmonization of data governance helps establish consistency across the continent. In 2022, the African Union took a significant step toward creating a consolidated data environment and harmonized digital data governance systems with its endorsement of the African Union Data Policy Framework. As an extensive blueprint, the framework is designed to guide African countries' efforts in developing data governance policies and legislative frameworks that align with the continent's unique contextual and capacity challenges (African Union 2023). Taking into consideration the various legal and regulatory environments, as well as different levels of maturity, the framework draws from the Digital Transformation Strategy (2020–2030) and the African Union's Agenda 2063, which, in turn, build on other continental digital policies developed to foster the advancement of digital technologies on the continent, such as the frameworks on the African Free Trade Area, personal data protection cybersecurity (the Malabo Convention) and child protection. The policy framework's guiding principles include cooperation, integration, fairness and inclusiveness, trust, safety and accountability, and sovereignty (Collaboration on International ICT Policy for East and Southern Africa 2022). It sets out guidelines for developing national laws protecting personal data and promoting data portability across borders. Specifically, the objectives of the framework are to enable the coordination of data governance, facilitate cross-border flows while promoting an equitable distribution of benefits and addressing risks, establishing trust mechanisms among member states, and enabling multi-stakeholder coordination to realize a single digital market (African Union 2023). Accordingly, domestication of the framework and implementation of its key recommendations at regional, national and continental levels will position Africa as a strong partner in the global economy and society (ibid.).

Another landmark framework is the African Union's Convention on Cyber Security and Personal Data Protection (2014), also known as the Malabo Convention, which requires states to implement domestic laws for personal data protection. Seeking to expand and harmonize data protection legislation, the convention aims to create a comprehensive legal framework for electronic commerce, data protection (including for automated processing of personal information), cybercrime and cybersecurity on the continent. As the continent's first legal instrument pertaining to digitalization, the Malabo Convention provides a framework similar to the European Union's General Data Protection Regulation and is considered to be "the only cybersecurity convention in the world that combines cybersecurity, cybercrime, electronic transactions, and data protection in one legal instrument" (Carnegie Endowment for International Peace 2023). At least 15 African states have adopted the Malabo Convention (African Union 2023). It is expected that all African Union member states party to the convention will be mandated to have domestic laws in each of the policy areas outlined in the convention. This will streamline data protection standards, eliminating the need for additional legal hurdles in cross-border data transactions (Thaldar 2023). It is anticipated that the convention can also be leveraged to facilitate the establishment of mutual legal assistance treaties that member states can use to exchange information on cyber incidents and share reporting on cybercrimes, bolstering the protection of personal information and mitigating

identity theft in e-commerce and cross-border transactions (Carnegie Endowment for International Peace 2023).

Finally, also emphasizing unified national approaches to development-focused and ethical artificial intelligence (AI) is the African Union's most recently endorsed and adopted instrument, the Continental AI Strategy (2024). The strategy is a comprehensive framework designed to guide the ethical and responsible development of AI technologies across Africa in achieving the Sustainable Development Goals and Agenda 2063 (African Union 2024). Currently, only six African countries have AI strategies (Okolo 2024). It is expected that aligning national policies to the strategy will help ensure that AI advances reflect data sovereignty, as well as African values and priorities, and the equitable distribution of benefits (African Union Development Agency-New Partnership for Africa's Development 2024). Calling for a multi-tiered governance approach involving a variety of stakeholders, the strategy proposes recommendations and action items for focusing on AI applications in sectors that harness benefits for African people, addressing the risks associated with the increasing use of AI — with particular attention to human rights, accelerating African Union member state AI capabilities and resources in digital infrastructure, and fostering regional and international cooperation to develop national AI policies by integrating them into national development plans (African Union 2024).

While representing significant steps in data governance, these instruments face much criticism around efficiency and implementation, leading to calls for revamping them (Okolo 2024) and updates through guidance notes and additional protocols (Carnegie Endowment for International Peace 2023). The Data Policy Framework is noted for its lack of coherence with regard to data ownership (Thaldar 2023), while the Malabo Convention is criticized for its vague definitions of important concepts with grave cross-border implications, such as data protection authority, pseudonymization and cross-border processing (Babalola 2022). Furthermore, as the African Union is an intergovernmental organization, and not supranational, its standards are non-binding. African states have sovereign rights to promulgate data protection legislation as they deem appropriate (Townsend 2021). However, as will be demonstrated in the next section, regional approaches to data governance help enhance interoperability and harmonization of national data regulations.

Implementation Challenges

While legislative frameworks are gaining traction in Africa, lawmakers often rush into creating the frameworks without adequate planning, leading to problems in implementation (Andere and Kathure 2024, 2). This is evidenced by the number of conventions that have not been ratified. For example, while the Malabo Convention was adopted in 2014, it only became enforceable in 2023 when the fifteenth member state ratified it, having finally reached the minimum number of countries required. The convention has yet to be ratified by all African Union member states amid concern over whether the instrument is still fit for purpose given the diffusion of emerging digital technologies since its adoption in 2014 (Carnegie Endowment for International Peace 2023).

There are several reasons for implementation challenges regarding digital frameworks, including inadequate resources (both human and financial), strong political will, misunderstanding the implications for local decision making, and variances in national data policies. According to Kunle Balogun and Adedeji Adeniran (2024), factors such as inappropriate or harmful exclusions carved into policies and the operative political system — given that non-democratic regimes are prone to be more restrictive on data flows and show a preference for data localization — can lead to variances in national data policies.

Concern over these variances in national data regulations is significant, especially regarding emerging technologies such as AI. As data plays a fundamental role in AI development, data protection legislation is the only form of governance currently in effect in several African countries that lack AI regulation.[2] However, Amba Kak and Rashida Richardson (2020) have argued that blind spots can be created when viewing AI regulation solely through a prism of data protection. Demonstrating how the "distinction between personal and non-personal data often crumbles under the realities of how data is generated and applied in AI technologies," Kak and Richardson highlight the limitations of data protection laws when apparently anonymous and discrete data is often combined using AI to reveal personal information, which leads to algorithmic profiling and exploitation (ibid.). Given projections that AI could expand the African GDP to US$1.5 billion by 2030 (Ngila 2022), the dominance of the financial technology and mobile money industry in the continent's digital finance ecosystem (Carnegie Endowment for International Peace 2023) and increased awareness of data protection rights, the need for harmonization in the advancement of data and AI regulation is apparent.

Case Studies

The effect of variances in data protection legislation oversight can be demonstrated through Bridget Andere and Megan Kathure's (2024) comparative case study of Kenya and South Africa regarding automated decision-making (ADM) technologies. ADM technologies such as those used in biometric identity databases entail heightened surveillance, thereby exacerbating the potential for inequality and discrimination. The Kenyan Data Protection Act requires data controllers to inform data subjects about the use and purpose of the collection of personal data. However, Andere and Kathure observe that the duty to inform data subjects is limited: data subjects are only notified when it is practicable for data controllers or processors. The authors recommend that data regulators should pay attention to how corporate and state actors can transgress accountability mechanisms in regulatory instruments. This can be done by requiring human rights impact assessments and by building in safeguards for non-discrimination and accountability (ibid., 16). In Kenya's Data Protection Act, non-discrimination is addressed through regulation 22(2)(h), which requires data controllers and processors to ensure that personal data is processed in a way that eliminates discriminatory effects and biases.

South Africa's data protection law, the Protection of Personal Information Act (POPIA)[3] also prescribes the conditions for lawful processing of personal information and ADM,

2 See https://dataprotection.africa.

3 *Protection of Personal Information Act* (S Afr), No 37067 of 2013, online: <https://popia.co.za/>.

giving data subjects the right to the lawful processing of their personal information. South Africa's data protection law is similar to that of Kenya regarding its addressing concerns about transparency and accountability. Where they differ, however, is that South Africa's POPIA makes no explicit demand for the elimination of discriminatory effects and bias in the processing of personal data and also does not require a data protection impact assessment. According to Andere and Kathure (2024), POPIA's limitations can be addressed by amending data protection laws to make provisions for specificity regarding exemptions, and by ensuring that mechanisms are in place to prevent governments or corporations from evading privacy rights (ibid., 16).

It has been argued that variances in national data protection regulation have negatively impacted timely access to the cross-border exchange of information. In her study of the impact of data regulation in the context of public health emergencies, Townsend (2021) draws on the COVID-19 pandemic to demonstrate the challenges in balancing the need for timely access to quality information and the exchange of personal health-related data with privacy principles. Townsend examines how South Africa's POPIA "travels with the data" by placing certain restrictions on the distribution and sharing of data both in the country and beyond its borders (ibid., 24).

Specifically, section 72 of POPIA provides for transborder data flows by containing requirements for the transfer of personal information and for the cross-border transfer of "special personal information." The transfer of personal information to a third party in a foreign country is only permitted where the legal grounds for such a transfer exists. These legal grounds include:

- the third party being subject to a law, binding corporate rules or a binding agreement that provides an adequate level of protection reflecting the principles of POPIA;
- the data subject consenting to the transfer;
- the transfer being necessary for the performance of a contract between the data subject and the responsible party;
- the transfer being necessary for the conclusion or performance of a contract concluded in the interest of the data subject; or
- the transfer benefiting the data subject.

An adequacy assessment is typically required in data protection provisions whereby the recipient country would need to have thresholds of data protection laws that are equivalent or substantially similar to the country from which the data was transferred. According to Townsend (2021), several African countries are not considered as being compliant with the "adequacy" standards of the European Commission, prompting proposals for the application of mechanisms such as standard contractual clauses, data trusts or the establishment of a data corridor as supplements or additional guarantees in cross-border data transfers. Townsend further highlights the need for greater regional integration and collaboration that will enable harmonizing national data regulations to promote the safe and lawful flow of personal information on the continent.

Recommendations

A sound data governance framework is one in which all stakeholders have the right incentives to produce, protect and share data (Ndemo and Thegeya 2022). To this effect, this paper holds the following recommendations:

- While aligning with international best practices, it is crucial that African nations develop data governance policies tailored to their unique contexts. Blindly adopting EU-style regulations, termed the "Brussels Effect" (Bradford 2019), may stifle innovative approaches that better reflect African realities and needs. In order for harmonization to succeed, the diverse populations, technological advancement levels and development goals of African states need to be key considerations.
- Cross-border data flows raise issues of sovereignty, privacy and security. The implementation of continental frameworks should be guided by actionable and practical intended outcomes that allow states to balance national security interests with the need for protecting data privacy.
- Meaningfully engage local stakeholders by inviting them to participate in advisory bodies and expert groups to enhance data stewardship. This can be strengthened further by developing multi-stakeholder African centres of excellence in data governance to provide the technical expertise, capacity building and pooling of resources to implement robust data governance frameworks.

Conclusion

Harmonizing data governance across Africa is a challenging yet crucial task in facilitating regional integration and economic growth. If done correctly, it offers the potential to unlock the benefits of the digital economy while protecting the shared values, rights and interests of Africans. However, this goal demands multi-stakeholder collaboration, sustained commitment and innovation in order for it to be achieved.

This paper uses the implementation challenges and gaps identified in key data governance frameworks in the region to help inform recommendations for policy makers and other stakeholders in Africa and beyond. The framework aims to enable the coordination of cross-border data flows, address risks, establish trust mechanisms among stakeholders and facilitate the creation of a single digital market. But it faces challenges and criticism, including a lack of coherence, vagueness and inadequate guidance and resources to implement it. Despite these limitations, the existing initiatives represent significant steps toward harmonizing data governance in Africa, potentially positioning the continent as a stronger partner in the global digital economy.

Acknowledgements

I would like to thank Alex He, Laila Mourad, J. Andrew Grant and Nanjala Nyabola for their guidance and invaluable comments on earlier drafts of this paper. I would also like to thank CIGI and the Digital Policy Hub for their program and curriculum that have stimulated engaging conversations and helped guide the direction of this research project.

About the Author

Badriyya Yusuf is a Social Sciences and Humanities Research Council doctoral candidate in international relations in the Department of Political Studies at Queen's University, Canada. She holds a master's degree in development practice from the University of Winnipeg. Badriyya adopts an interdisciplinary approach to global digital governance, political economy and international development. Her recent work on regional security governance has been published by Routledge and *International Journal*. Her research as a doctoral fellow with the Digital Policy Hub will examine data governance frameworks, with a focus on Sub-Saharan Africa.

Works Cited

Aaronson, Susan Ariel. 2018. *Data Is Different. Why the World Needs a New Approach to Governing Cross-border Data Flows*. CIGI Paper No. 197. Waterloo, ON: CIGI. www.cigionline.org/static/documents/documents/paper%20no.197_0.pdf.

African Union. 2023. "List of Countries Which Have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection." May 12. https://dataprotection.africa/wp-content/uploads/2305121.pdf.

– – –. 2024. *Continental Artificial Intelligence Strategy: Harnessing AI for Africa's Development and Prosperity*. July. https://au.int/en/documents/20240809/continental-artificial-intelligence-strategy.

Andere, Bridget and Megan Kathure. 2024. *Strengthening Data Protection in Africa: Key Issues for Implementation*. Access Now. January. www.accessnow.org/wp-content/uploads/2024/01/Strengthening-data-protection-in-Africa-key-issues-for-implementation-updated.pdf.

African Union Development Agency-New Partnership for Africa's Development. 2024. "Shaping Africa's Artificial Intelligence (AI) Strategies." August 26. www.nepad.org/news/shaping-africas-artificial-intelligence-ai-strategies.

Babalola, Olumide. 2022. "Data Protection Legal Regime and Data Governance in Africa: An Overview." African Economic Research Consortium Policy Brief No. DG003. February. https://aercafrica.org/old-website/wp-content/uploads/2022/02/DG003.pdf.

Balogun, Kunle and Adedeji Adeniran. 2024. "Towards A Sustainable Regional Data Governance Model in Africa." Policy brief. Centre for the Study of the Economies of Africa. June. https://cseaafrica.org/images/posts/7332684359831731.pdf.

Bradford, Anu. 2019. *The Brussels Effect: How the European Union Rules the World*. Oxford, UK: Oxford University Press.

Carnegie Endowment for International Peace. 2023. "Continental Cyber Security Policymaking: Implications of the Entry Into Force of the Malabo Convention for Digital Financial Systems in Africa." Virtual event, July 10. https://carnegieendowment.org/events/2023/07/continental-cyber-security-policymaking-implications-of-the-entry-into-force-of-the-malabo-convention-for-digital-financial-systems-in-africa.

Collaboration on International ICT Policy for East and Southern Africa. 2022. "Five Takeaways from the 2022 African Union Data Policy Framework." Policy brief. October. https://cipesa.org/wp-content/files/briefs/Five_Takeaways_From_the_2022_African_Union_Data_Policy_Framework_Brief.pdf.

CSM. 2024. "Focusing on Effective Data Governance in Africa." CSM (blog), April 26. www.csm.tech/blog-details/focusing-on-effective-data-governance-in-africa/.

Internet & Jurisdiction Policy Network. 2022. *Framing, Mapping & Addressing Cross-Border Digital Policies in Africa: An Internet & Jurisdiction Policy Network Regional Status Report.* www.internetjurisdiction.net/uploads/ pdfs/Executive-Summary-Crossboder-Digital-Policies-in-Africa.pdf.

Kak, Amba and Rashida Richardson. 2020. "Artificial Intelligence Policies Must Focus on Impact and Accountability." Opinion, Centre for International Governance Innovation, May 1. www.cigionline.org/articles/artificial-intelligence-policies-must-focus-impact-and-accountability/.

KPMG. 2023. "Nigeria Data Protection Act 2023 Review." August. https://assets.kpmg.com/content/dam/kpmg/ng/pdf/nigeria-data-protection-act2023_kpmg-review.pdf.

Ladley, John. 2019. *Data Governance: How to Design, Deploy, and Sustain an Effective Data Governance Program*. New York, NY: Elsevier.

Ndemo, Bitange and Aaron Thegeya. 2022. "A Data Governance Framework for Africa." African Economic Research Consortium Policy Brief No. DG001. February. Nairobi, Kenya: African Economic Research Consortium. https://africaportal.org/wp-content/uploads/2023/06/DG001.pdf.

Ngila, Faustine. 2022. "Africa is joining the global AI revolution." Quartz, June 23. https://qz.com/africa/2180864/africa-does-not-want-to-be-left-behind-in-the-ai-revolution.

Okolo, Chinasa T. 2024. "Reforming data regulation to advance AI governance in Africa." Brookings, March 15. www.brookings.edu/articles/reforming-data-regulation-to-advance-ai-governance-in-africa/.

Thaldar, Donrich. 2023. "Harmonizing Africa's Data Governance: Challenges and Solutions." *Bill of Health* (blog), November 6. https://blog.petrieflom.law.harvard.edu/2023/11/06/harmonizing-africas-data-governance-challenges-and-solutions/.

Townsend, Beverley. 2021. "The lawful sharing of health research data in South Africa and beyond." *Information & Communications Technology Law* 31 (1): 17–34. https://doi.org/10.1080/13600834.2021.1918905.

World Bank Group. 2020. *The African Continental Free Trade Area: Economic and Distributional Effects*. July 27. Washington, DC: World Bank Group. www.worldbank.org/en/topic/trade/publication/the-african-continental-free-trade-area.

Yusuf, Badriyya. 2024. "Sustainable Data Governance Frameworks in Africa." Digital Policy Hub Working Paper. www.cigionline.org/static/documents/DPH-paper-Yusuf.pdf.