Operationalizing Comprehensive Data Governance in Africa

CHINASA T. OKOLO

Fellow, The Brookings Institution
Email: cokolo@brookings.edu

Abstract

The increasing development of machine learning (ML) models and adoption of artificial intelligence (AI) tools, particularly generative AI, has dramatically shifted practices around data, spurring the development of new industries centered around data labeling and revealing new forms of exploitation, including illegal data scraping for AI training datasets. These new complexities around data production, refinement, and use have also impacted African countries, elevating a need for comprehensive regulation and enforcement measures. While 38/55 African Union (AU) Member States have existing data protection regulations, there is a wide disparity in the comprehensiveness and quality of these regulations and in the ability of individual countries to enact sufficient protections against data privacy violations. Thus, to enable effective data governance, AU Member States must enact comprehensive data protection regulations and reform existing data governance measures to cover aspects such as data quality, privacy, responsible data sharing, transparency, and data worker labor protections. This paper analyzes data governance measures in Africa, outlines data privacy violations across the continent, and examines regulatory gaps imposed by a lack of comprehensive data governance to outline the sociopolitical infrastructure required to bolster data governance capacity. This work introduces the RICE Data Governance Framework, which aims to operationalize comprehensive data governance in Africa by outlining best measures for data governance policy reform, integrating revamped policies, increasing continental-wide cooperation in AI governance, and improving enforcement actions against data privacy violations.

Keywords: Data privacy, data governance, policy reform, African development, artificial intelligence

Introduction

The advent of generative artificial intelligence (AI), increasing adoption of AI tools, and the widespread utilization of data workers have changed narratives around data production and use. While data protections exist in 38 out of 55 African Union (AU) Member States, intensifying algorithmization across Africa could impact users through digital platforms used to access education, healthcare, financial, and social services. Given these new complexities and the emerging AI regulatory environment within the continent, African governments must enact comprehensive data protection regulations and reform existing data governance measures to cover aspects such as data quality, privacy, responsible data sharing, transparency, and data worker labor protections. To address these issues, data workers in Kenya have pursued litigation against Facebook regarding subpar working conditions and unfair termination (Musanga, 2023), and data workers across the continent have established organizations such as Techworker Community Africa (TCA)[1], the African Content Moderators Union, the Nigerian Content Moderators and Tech Workers Union (NCMTW)[2], and the Kenyan Content Moderators' Union. Along with general subpar working conditions across the continent in fields such as oil production and garment manufacturing, the concerns imposed by data work underscore requirements for sectoral reform of existing labor protections in areas including agriculture, economics, education, and healthcare. African countries also have context-specific challenges that differ significantly from those within the West, highlighting a need to understand how to develop culturally aligned and feasible governance solutions (Okolo, 2023).

By balancing lessons from the recent ratification of the African Union Convention on Cyber Security and Personal Data Protection, maturing regulatory environments like the EU, and advancing research on regional and country-specific needs, African nations can work towards more robust regulation. This paper analyzes data governance measures in Africa, outlines data privacy violations across the continent, and examines

[1] https://techworkercommunityafrica.org/

[2] https://www.linkedin.com/company/nigerian-content-moderators-acmu/

regulatory gaps imposed by a lack of comprehensive data governance to outline the sociopolitical infrastructure required to bolster data governance capacity. Additionally, it proposes the RICE Data Governance Framework, which African national governments (NGs), Regional Economic Communities (RECs), and the African Union can leverage to reform and operationalize existing data protection measures. Ultimately, this framework could inform the development and implementation of context-specific AI regulation that centers data privacy rights.

Data Governance in Africa

The increasing development and adoption of AI have dramatically shifted practices around data, spurring the development of new industries and revealing new forms of exploitation. These new complexities around data production, refinement, and use have also impacted African countries, elevating a need for comprehensive governance and enforcement measures. Approximately 38 out of 55 African Union Member States have enacted formal data protection regulations. 15 out of 38 data protection laws passed by African countries were enacted in the last five years, and 26 were enacted in the last decade. The first data protection law in Africa was enacted by Cabo Verde in 2001, and data protection laws were recently enacted by Malawi in June 2024 and Ethiopia in July 2024. As of October 2024, Namibia, South Sudan, and The Gambia have drafted data protection laws yet to be enacted.

National Data Governance Efforts

Nigeria launched the National Data Protection Act (NDPA) in June 2023. This Act was preceded by the National Data Protection Regulation (NDPR) issued by the Nigerian National Information Technology Development Agency (NITDA) in January 2019. The primary objective of the NDPA is to "safeguard the fundamental rights and freedoms, and the interests of data subjects" in Nigeria by regulating personal data processing, protecting the rights of data subjects, and ensuring that data controllers and processors are in line with the Act. The Act restricts cross-border data transfers and gives data subjects the right to object to data collection, withdraw consent from data processing, and object to automated decision-making.

Senegal introduced data privacy regulation relatively early compared to other African countries, publishing Act No 2008-12 Concerning Personal Data Protection on January 25, 2008, and implementing Decree No 2008-721, the Personal Data Protection Act on 30 June 2008. This law requires data subjects to be notified about data processing and consent to data transfers. The Senegal Personal Data Protection Commission (CDP) is the governing body responsible for ensuring that all data processing within the country complies with the Data Protection Act.

Egypt introduced the Law on the Protection of Personal Data issued under Resolution No. 151 of 2020, published in July 2020, and took effect in October 2020. This law requires obtaining consent from data subjects before processing personal data. It also gives rights to data subjects, which include knowledge of what personal data is being processed and by whom, the ability to withdraw consent to data processing, the ability to correct, modify, delete, or update personal data, and be informed regarding personal data breaches. This law also prohibits the transfer of personal data outside of Egypt to countries with insufficient data protections unless direct consent is obtained from a data subject or their representatives.

Rwanda passed legislation covering data privacy and protection in 2021, which ratified Law No. 058/2021 of 13 October 2021, Relating to the Protection of Personal Data and Privacy. This law contains 70 articles that cover the processing and quality of personal data, the rights of data subjects, and the sharing, transfer, storage, and retention of personal data. All organizations that collect or process data were required to be in compliance with this law by October 15, 2023, two years after the law was initially enacted.

Continental and Regional Data Protection Efforts

Along with country-specific data governance regulations, regional entities such as the African Union (AU) and the Economic Community of West African States (ECOWAS) have introduced data protection acts. The AU Malabo Convention, also known as the African Union Convention on Cyber Security and Personal Data Protection, was ratified in June 2023, nine years after its adoption. It was drafted in 2011 at the 17th Ordinary African Union Summit in Malabo, Equatorial Guinea, adopted by the African Union in 2014, and entered into force on June 8, 2023, after being ratified by

Mauritania, the 15th country needed for ratification to officially "be in force." It aims to establish comprehensive norms and regulations for cybersecurity and data privacy across the African continent. The Malabo Convention establishes criminal sanctions for various cybercrimes, including data breaches and attacks on computer systems. It requires data protection measures for the collection, storage, and processing of personal data, upholding individual privacy rights. It also aims to promote electronic commerce by fostering a secure and trustworthy online environment for transactions and encourages collaboration among AU Member States for information sharing, capacity building, and coordinated responses to cyber threats.

The Economic Community of West African States (ECOWAS) is a regional political and economic union of fifteen countries located in West Africa. It was established on May 28, 1975, with the signing of the Treaty of Lagos, and aims to promote economic integration across the region. The ECOWAS Supplementary Act on Personal Data Protection was signed by The Authority of Heads of State and Government of ECOWAS on 16 February 2010 in Abuja, Nigeria. The Act outlines requirements for Member States to establish their respective data protection authorities and the required content Member States should incorporate into their data privacy laws. Overall, it aims to establish coordinated legal frameworks for personal data processing. Out of the 15 Member States, 9 (Benin, Burkina Faso, Cape Verde, Ghana, Ivory Coast, Niger, Nigeria, Senegal, and Togo) have implemented data protection laws.

Other continental efforts towards data protection have been spearheaded by the Southern African Development Community (SADC), an intergovernmental organization that aims to achieve regional integration and promote socioeconomic development across its 16 Member States: Angola, Botswana, Comoros, Democratic Republic of Congo, Eswatini, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, United Republic of Tanzania, Zambia and Zimbabwe. In 2013, the SADC passed the Model Law on Data Protection to provide a guiding framework for Member States to establish data protection regulations (ITU Telecommunication Development Bureau, 2013). The East African Community (EAC) is a regional intergovernmental organization promoting economic, political, and social cooperation between Burundi, the Democratic Republic of Congo, Kenya, Rwanda, Somalia, South Sudan, Tanzania, and Uganda. In 2008, EAC drafted the Legal Framework for Cyberlaws, which outlined steps towards digital regulation and data governance amongst EAC Member States (East African Community, 2008). At the moment, there have been no regional governance measures proposed or enacted by the Arab Maghreb Union (AMU), the Community of Sahel–Saharan States (CEN–SAD), and the Economic Community of Central African States (ECCAS).

Many regional efforts towards developing digital policies and frameworks across the continent were supported by the "Harmonization of the ICT Policies in Sub-Sahara Africa" (HIPSSA) Project (Bazzanella & Bihan, 2012). HIPSSA was launched in 2008 and supported by the International Telecommunication Union (ITU) and the European Commission, following previous regional harmonization efforts supported by the African Development Bank, European Union (EU), ITU, U.S. Agency for International Development (USAID), the Organisation Internationale de la Francophonie (OIF), and the United Nations Economic Commission for Africa (UNECA).

Data Regulatory Gaps in Africa

Prior research has examined the data regulatory environment in Africa, uncovering numerous systematic gaps hindering responsible and sustainable data governance throughout the continent (Eke *et al.*, 2022). Eke *et al.* specifically examine data governance approaches in five African countries, Kenya, Mauritius, Morocco, Nigeria, and South Africa, finding issues with compliance and enforcement of existing protections and a lack of data governance structures within the public and private sectors. The rising adoption of AI tools has also introduced gaps within existing data protection regulations that could be further exploited as AI development increases throughout the continent. While companies have traditionally leveraged consumer data to improve ad targeting and personalized recommendations, companies are now leveraging existing consumer data to train AI tools. Over the past few years, there has been a rise in the number of AI clauses introduced into terms of service (ToS) agreements, giving companies the right to incorporate consumer data into datasets to train proprietary AI models. Recent cases include Zoom changing their ToS to leverage "customer content" and "service generated data" to train and test AI tools in March 2023. After backlash on social media in August 2023, Zoom altered the new AI clauses to indicate that such data is not used to train models without customer consent (Rakova, 2023). Other companies like Meta have introduced AI clauses providing them with the ability to use customer data for AI, but these changes are also complicated by the lack of opt-out choices from consumers in regions where there are insufficient data protection laws (Diaz, 2024).

To quell issues around intellectual property theft, prominent AI companies like OpenAI have announced a series of partnerships with social media companies like Reddit and media outlets such as TIME, The Atlantic, News Corp, the Associated Press, Vox Media, Financial Times, BuzzFeed, and others (Simmonds, 2024). However, these increasing partnerships are raising antitrust concerns from regulators within the EU and the United States (Federal Trade Commission, 2024; Chee, 2024). While no significant partnerships have been announced between OpenAI and African organizations, many of these media companies have offices in African countries. African users also access and actively use social media platforms that have forged partnerships with OpenAI. However, a recent partnership between Liquid Technologies, an African cloud service provider headquartered in Mauritius, Google Cloud, and Anthropic potentially indicates future diversification in big tech AI partnerships (Liquid Intelligent Technologies, 2024). With this in mind, African regulatory bodies must also examine the impact of foreign antitrust probes in local markets and bolster enforcement capacity.

Data Privacy Violations in Africa

Existing data regulatory gaps may also contribute to the growing number of data privacy violations experienced across Africa. In March 2023, the Angolan Agência de Protecção de Dados (APD) issued a fine to Africell, an electronic communications operator, who collected personal consumer data without requesting prior authorization from APD (Agência de Protecção de Dados, 2023). In November 2023, the Telecommunications/ICT Regulatory Authority of Côte d'Ivoire (ARTCI) issued a formal warning to YANGO, a local ridesharing application, for unlawfully recording passenger phone conversations (l'ARTCI, 2023). In July 2023, the South African Information Regulator issued a ZAR 5 million (~USD 273,000) fine against the Department of Justice and Constitutional Development for failure to implement adequate security measures to prevent a ransomware attack in 2021 and noncompliance with required consumer notifications regarding the subsequent data breach (Information Regulator South Africa, 2023). One of the continent's most recent data privacy violations involves a data breach of Nigeria's National Identity

Management Commission of Nigeria (NIMC) system, which has resulted in millions of data points being available for sale on illicit websites for NGN 100, which is about USD 6 cents (Paradigm Initiative, 2024). As of July 2024, it is unclear what action the Nigeria Data Protection Commission has taken against the offenders. Kenya Office of the Data Protection Commissioner (ODPC) issued multiple penalties to 4 companies in 2023, totaling over KES 14 million. These fines included noncompliance with a prior enforcement notice on spam calls, harassment from microlending apps, posting minor images, and using customer photos for marketing. ODPC has also made progress in an ongoing investigation regarding violations by Worldcoin, an American cryptocurrency provider that undertook biometric data collection without government notice (Communications Authority Kenya, 2023). While African data protection agencies have increasingly taken actions toward enforcing data protection laws, there is still little understanding of how effective these measures are, given frequent noncompliance with enforcement notices (Lawyers Hub, 2024) and little information on fine payments by offenders.

Operationalizing Data Governance in Africa

In order to ensure that African countries can effectively protect consumers against improper data practices and enforce corrective action against data privacy violations, African governments across every AU Member State must enact comprehensive data regulatory measures. While existing continental-wide efforts, such as the African Union Data Policy Framework, which was published in 2022 to guide AU Member States in designing and reviewing data regulations, and the Malabo Convention on Cyber Security and Personal Data Protection, offer valuable templates for African governments to adopt, these frameworks have unfortunately not seen wide adoption. To help address this lack of adoption and potential challenges from data regulatory gaps, a number of proposals have outlined alternative measures, including regional data governance approaches (Osakwe & Adeniran, 2021; Balogun & Adeniran, 2024), community-centered governance models (Olorunju & Adams, 2024), and data governance reformation (Okolo, 2024). This section introduces the RICE Data Governance Framework to provide a high-level overview of actions African Union Member States can leverage to operationalize data governance effectively.

Reformation, Integration, Cooperation, & Enforcement (RICE) Framework

In lieu of functional continental frameworks, countries, regional, and continental bodies should focus on (1) **reforming** existing data regulation and implementing sectoral policy reformation, (2) collaborating with Civil Society Organizations (CSOs) and Academic Research Institutions (ARIs) to improve **integration** of reformed policies, (3) increasing regional and continental **cooperation** in data regulation efforts, and (4) strengthening **enforcement** of reformed data regulation. The RICE Data Governance Framework recommendations apply at the national, regional, and continental levels.

To begin operationalizing the RICE Data Governance Framework, African governments should pursue regional data governance measures, given the lack of existing coordination with and insufficient protections within existing continental measures such as the Malabo Convention (Yilma, 2022; ALT Advisory, 2022; Balogun & Adedeji, 2024). Efforts to pursue regional data governance would ideally be led by existing RECs such as ECOWAS, EAC, SADC, AMU, CEN-SAD, and ECCAS. Such efforts can then enable the 19 African Union Member States without existing data protections to draft and enact comprehensive data governance measures in a reasonable timeframe. Additionally, enacting regional data governance policies can help address existing capacity constraints for AU Member States unable to individually draft and enact data legislation.

Reformation

To address concerns regarding a lack of comprehensive data governance measures, the AU, RECs, and individual African NGs must reform existing data governance measures and engage in sectoral policy reform.

- The AU, RECs, and NGs should review existing data protection measures, leveraging SWOT analysis methods to understand gaps. To meet data governance needs, they should subsequently reform sectoral policies in agriculture, economics, education, healthcare, and other areas.
- The AU must establish a convention specific to data protection by leveraging the AU Data Policy Framework and refining data protection clauses from the Malabo Convention.

- The AU, RECs, and NGs must harness the capabilities of their digital ministries (DMs) by establishing local expert groups and advisory bodies.
- DMs should leverage participatory policy development approaches by consulting local expert groups, collaborating with government agencies, and soliciting input from the general public to enhance policy reform.
- The AU, RECs, and NGs should periodically iterate and engage in policy reform to ensure that standards align with present-day practices.

Integration

To increase awareness and local integration of data protection regulation, RECs and NGs will need to improve outreach to organizations under their jurisdiction. RECs and NGs should also fund outreach and research efforts by CSOs and ARIs to improve public engagement with data protection measures.

- RECs and NGs should send accessible, comprehensive, and timely notices to organizations, informing them of data policy reforms.
- RECs and NGs should lead efforts to establish a Data Protection, Governance, and Compliance Officers database to improve institutional outreach.
- CSOs and ARIs should develop data literacy training for citizens to increase public understanding of data rights.
- CSOs should advocate for citizens with affected rights and leverage their capacity to inform RECs and NGs about data privacy violations.
- ARIs and CSOs should conduct in-depth research that advances understanding of regional and country-specific needs for data regulation and reduces reliance on standards such as the EU General Data Protection Regulation (GDPR).

Cooperation

To address issues regarding a lack of regional cooperation and inconsistencies in data protection regulation, the AU must lead harmonization efforts across AU Member States. To mitigate issues with prior harmonization efforts, the AU should actively consult RECs and NGs in harmonization efforts (Kenyanito & Chima, 2016).

- The AU must develop a Data Governance Harmonization Body, building upon prior efforts such as HIPSSA.
- When developing the Body, the AU should prioritize multistakeholder input from RECs and NGs and actively communicate with these stakeholders.
- The AU should establish a continental-wide network of National Data Protection Authorities and Offices (NDPAs/NDPOs), as previously recommended (Data Protection Africa, 2023).

Enforcement

To help address concerns regarding a lack of enforcement of data protection measures, the AU must establish a continental data supervisory body. African governments must also leverage data protection offices to enforce enacted regulations.

- The AU should inaugurate a Data Protection Supervisory Authority (DPSA) to increase regional enforcement for data privacy violations and help RECs and NGs enforce regulations.
- The AU and RECs should help NGs establish NDPAs and NDPOs to mitigate regulatory enforcement gaps.
- The AU DPSA should collaborate with RECs and NDPAs/NDPOs to develop standards to maintain best operating practices that will increase compliance with enforcement notices and fine payment.
- The AU should leverage the DPSA to continually monitor the activities of the continental NDPA/NDPO network and serve as an arbitrator for disputes.

Considerations

While this data governance operationalizing framework aims to ease the implementation of comprehensive data regulation within African countries, many considerations exist for the ability of all governments across the continent to leverage this framework. Existing issues with infrastructure, electricity access, education, digital skills literacy, skilled AI talent, climate change, armed conflict, social unrest, national security, and socioeconomic growth may deprioritize and sideline efforts toward data governance. In light of these existing challenges, however, governments must focus on developing culturally aligned and feasible data governance solutions to ensure that the data rights of African consumers are preserved and that there are adequate outlets for redress of data protection harms.

Regional data governance led by RECs would ideally take precedence over the AU until a formal continental-wide data protection law is passed. However, efforts will be needed to rectify duplicative membership within the RECs and integrate AU Member States without membership in RECs, like the Sahrawi Arab Democratic Republic, which controls the Western Sahara. Prioritizing regional-led data governance before continental reforms are enacted could help address capacity constraints and harmonization issues between AU Member States. Still, there is no guarantee that countries within RECs will reach alignment on data governance measures.

With the growing number of regional and national efforts toward AI regulation throughout the continent, African governments must also understand the fundamental role of data in training ML models, evaluating AI systems, refining predictive models, and improving AI-enabled services (GPAI Data Governance Working Group, 2020). Given these essential functions, efforts towards enacting effective data governance can also enable more comprehensive AI governance measures. Thus, African governments should consider comprehensive data governance as a viable pathway and complement to AI regulation. To bolster AI-related governance overall, it will also be crucial for African governments to invest in efforts to understand the diverse policy challenges associated with data, including privacy, transparency, labor, interoperability, discrimination, cross-border data flows, and intellectual property.

Conclusion

While the potential of AI is still nascent within Africa, African consumers hold valuable data that is subject to exploitation by both local and international firms alike. Companies are increasingly looking towards African countries to supply them with the necessary data to expand target markets for their AI services. With governments, companies, universities, and other institutions in African countries rapidly adopting AI technologies, there are also concerns that algorithmic harms primarily noted in Western contexts could be exacerbated in ways that disproportionately harm marginalized populations throughout the continent. The limited research examining concrete ethical concerns around data privacy and the lack of extensive efforts toward data protection in Africa is concerning. This work examines data governance measures in Africa, highlighting the regulatory gaps imposed by a lack of comprehensive data governance across Africa that could be further exploited by rising AI adoption. This work presents the RICE Data Governance Framework to operationalize comprehensive data governance in African Union Member States to reform and optimize existing data protection measures while bolstering Africa's emerging AI regulatory environment.

Bibliography

Agência de Protecção de Dados (APD). (2023). APD multa AFRICELL em 150 mil dólares norte americanos por violação da Lei de Protecção de Dados Pessoais (LPDP). https://www.apd.ao/ao/noticias/apd-multa-africell-em-150-mil-dolares-norte-americanos-por-violacao-da-lei-de-proteccao-de-dados-pessoais-lpdp/.

ALT Advisory. (2022). The Malabo Roadmap: Approaches to promote data protection and data governance in Africa. Mozilla. https://dataprotection.africa/wpcontent/uploads/malabo_roadmap_Sept_2022.pdf.

Balogun, K., & A. Adeniran (2024). Towards A Sustainable Regional Data Governance Model in Africa. Centre for the Study of African Economies (CSEA).

Bazzanella, S., & J.L. Bihan (2012). Support for Harmonisation of ICT Policies in Sub-Sahara Africa Implementation Strategy. International Telecommunication Union.

Chee, F. Y. (2024). AI deals between Microsoft and OpenAI, Google and Samsung, in EU crosshairs. Reuters. https://www.reuters.com/technology/eu-seeks-views-microsoft-openai-google-samsung-deals-eus-vestager-says-2024-06-28/.

Communications Authority Kenya. (2023). CA and Data Commissioner Warn Kenyans Over Worldcoin. https://www.ca.go.ke/ca-and-data-commissioner-warn-kenyans-over-worldcoin.

Data Governance Working Group of the Global Partnership on AI (GPAI). (2020). The Role of Data in AI. GPAI. https://gpai.ai/projects/data-governance/role-of-data-in-ai.pdf.

Data Protection Africa, (2023). Africa: AU's Malabo Convention set to enter force after nine years. ALT Advisory. https://dataprotection.africa/malabo-convention-set-to-enter-force/.

Diaz, J. (2024). Instagram is training AI on your data. It's nearly impossible to opt out. Fast Company. https://www.fastcompany.com/

91132854/instagram-training-ai- on-your-data-its-nearly-impossible-to-opt-out.

East African Community, (2008). Draft EAC Legal Framework for Cyberlaws. http://repository.eac.int/handle/11671/1815

Eke, D., P. Ochang, A. Adimula, F. Borokini, S. Akintoye, R. Oloyede, L. Sorborikor, M. Adeyeye, B. Wale-Oshinowo and T. Ogundele (2022). Responsible Data Governance in Africa: Institutional Gaps and Capacity Needs. Centre for the Study of African Economies (CSEA).

Federal Trade Commission, (2024). FTC Launches Inquiry into Generative AI Investments and Partnerships. United States Government. https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-launches-inquiry-generative-ai-investments-partnerships

Information Regulator South Africa, (2023). Media Statement Infringement Notice and R5 Million Administrative Fine Issued to The Department of Justice and Constitutional Development for Contravention of Popia. https://inforegulator.org.za/wp-content/uploads /2020/07/MEDIA-STATEMENT-INFRINGEMENT- NOTICE- ISSUED-TO-THE-DEPARTMENT-OF-JUSTICE-AND-CONSTITUTIONAL.pdf.

International Telecommunication Union Telecommunication Development Bureau (BDT), (2013). Data Protection: Southern African Development Community (SADC) Model Law.

Kenyanito, E.P., and R.J.S. Chima (2016). Room for improvement: Implementing the African Cyber Security and Data Protection Convention in Sub-Saharan Africa. AccessNow.

l'ARTCI, (2023). Communiqué - l'ARTCI. https://www.artci.ci/index.php/33-actualites/informations/629-probables-enregistrements-des-communications-ou-echanges-a-l-interieur-de-vehicules-utilisateurs-de-l-application-denommee-yango-sans-information-prealable-ou-consentement-des-personnes-concernees.html.

Lawyers Hub, (2024). Africa Privacy Report 2023/2024. https://www.lawyershub.org/digital

Liquid Intelligent Technologies, (2024). Liquid C2 partners with Google Cloud and Anthropic to bring advanced cloud, cyber security and generative AI capabilities to Africa. https://za.liquid.tech/about-us/news/liquid-c2-partners-with-google-cloud-and-anthropic/.

Musanga, M. (2023). Facebook workers in Kenya say Meta hasn't paid them for 6 months amid legal case. openDemocracy. https://www.opendemocracy.net/en/facebook-workers-in-kenya-say-meta-hasnt-paid-them-for-6-months-amid-legal-case/

Ndemo, B., and A. Thegeya (2023). A Prototype Data Governance Framework for Africa. In Data Governance and Policy in Africa (pp. 9-29). Cham: Springer International Publishing.

Olorunju, N., and R. Adams (2024). African data trusts: new tools towards collective data governance? Information & Communications Technology Law, 33(1), 85-98.

Okolo, C.T. (2023). AI in the Global South: Opportunities and challenges towards more inclusive governance. The Brookings Institution.

Okolo, C.T. (2024). Reforming data regulation to advance AI governance in Africa. Foresight Africa 2024. The Brookings Institution. https://www.brookings.edu/articles/reforming-data-regulation-to-advance-ai-governance-in-africa/

Osakwe, S., and A. Adeniran (2021). Strengthening Data Governance in Africa. Centre for the Study of African Economies (CSEA).

Paradigm Initiative (2024). Major Data Breach: Sensitive Government Data of Nigerian Citizens Available Online for Just 100 Naira. https://paradigmhq.org/major-data-breach-sensitive-government-data-of-nigerian-citizens-available-online-for-just-100-naira/.

Perrigo, B. (2023). OpenAI Used Kenyan Workers on Less Than $2 Per Hour to Make ChatGPT Less Toxic. TIME. https://time.com/6247678/openai-chatgpt-kenya-workers/

Rakova, B. (2023). What The Zoom Controversy Teaches Us About AI and Consent. Medium. https://bobi-rakova.medium.com/if-you-continue-to-use-the-services-after-the-effective-date-of-the-changes-then-you-agree-to-the-52022856d771.

Salami, E. (2022). Implementing the AfCFTA agreement: a case for the harmonization of data protection law in Africa. Journal of African Law, 66(2), 281-291.

Saturday, B., and B. Nyamwire (2023). Towards Effective Data Governance in Africa: Progress, Initiatives and Challenges Policy.

Simmonds, R. (2024). OpenAI Partnerships List. Foundation Marketing. https://foundationinc.co/lab/openai-partnerships-list/

Yilma, K. (2022). African Union's data policy framework and data protection in Africa. Journal of Data Protection & Privacy, 5(3), 209-215.