Safeguarding Digital Rights & User Safety

Strengthening Data Governance in Africa

Developed under the Africa Data Governance Hub,
in collaboration with Pollicy and NIYEL.

Author: Abigail Adu-Daako.

Reviewed by Dr. Muhammad Aliyu Suleiman.

December 2024

Introduction

Africa’s rapid digital transformation offers significant opportunities for economic growth and societal progress, driven by increasing internet connectivity, expanding digital infrastructure, and emerging technologies. However, these advancements impact data privacy, user safety, and digital rights, particularly in countries with underdeveloped regulatory frameworks. Data governance has emerged as a cornerstone of the digital economy, yet, many African countries face significant gaps in their data governance frameworks, which hinder their ability to safeguard personal information, mitigate cybersecurity threats, and address the ethical challenges posed by AI. While 74% of African countries have data protection laws, enforcement remains weak, and some lack the specificity needed to address AI-related risks. These gaps underscore the urgency of robust, context-specific data governance policies that prioritize user safety and digital rights.

This policy paper examines the current state of data governance in Africa, focusing on the intersection of AI, digital rights, and user safety. It highlights specific gaps related to human rights and user safety and offers actionable recommendations for governments to enhance governance, prioritize user safety and digital rights, and build trust in the digital ecosystem.

Data evolution in Africa

The evolution of data has been transformative, driven by advances in digital technologies, including artificial intelligence (AI). The World Economic Forum estimates that by 2025, 463 exabytes of data will be generated daily,[1] underscoring the scale of the exponential growth of data in our digital age. Africa's data evolution mirrors global trends, though it has faced unique challenges such as limited digital infrastructure, low internet penetration, unreliable electricity, and low levels of digital literacy. Despite these challenges, significant progress has been made in the past decade. According to the World Bank, internet users in Sub-Saharan Africa increased by 115% between 2016 and 2021,[2] driven by improved access to mobile networks and broadband internet. Also by 2016, at least 10 African countries had established open data portals.[3] The fintech sector has seen remarkable advancements, with mobile money systems enabling digital transactions in over 20 African countries.[4] Governments are increasingly digitizing public services to improve governance,[5] while increased investments in data centers, broadband, and undersea cables have strengthened connectivity. Smartphone adoption, a key driver of data creation, is projected to reach 87% in Sub-Saharan Africa by 2030, signaling a continued acceleration in data generation and usage.[6]

Data Governance Progress, Gaps and Challenges in Africa

Data governance in Africa emerged as a response to the rapid digitization of communication and commerce, initially focusing on telecommunications and mobile financial services. Over time, this expanded to include personal data protection, cybersecurity, and ethical technology use. Cabo Verde led the way in 2001 with Africa's first data protection law. As of November 2024, 74% of African countries have enacted data protection laws, with one-third passed in the last five years. While the GDPR influenced several African policies, other regional frameworks such as the Malabo Convention on Cybersecurity and Personal Data Protection (2014) and the African Union Data Policy Framework (2022) (AU DPF) have also shaped the regulatory landscape.

Common provisions across African data protection laws include obtaining user consent, ensuring data minimization, and enabling user rights to access, correct, and delete data. There are also significant differences and gaps among these policies. Some require the creation of a Data Protection Authority (DPA), while others do not. Currently, about 8 countries have data protection laws with no assigned enforcement authorities,[7] for countries with a DPA, the lack of independence, inadequate funding, and insufficient capacity undermine their ability to hold entities accountable.[8] Some countries also have stricter penalties for violations than others. For example, South Africa's POPIA imposes fines of up to ZAR 10 million (~$500,000) or imprisonment for serious violations, whereas others have less severe fines and emphasize warnings and corrective measures over punitive actions. This diminishes the deterrent effect of penalties, coupled with a slow pace of legal proceedings, judicial backlogs, and inconsistent interpretation by courts.

Cross-border data transfers and data localization are also areas where key differences exist. While some countries such as Ghana, Gambia, and Liberia allow for data transfers, many others have stricter adequacy protections.[9] Regional frameworks like the AU DPF and the AfCFTA Digital Trade Protocol have emphasized the need for greater harmonization to facilitate cooperation and ease business operations across Africa. Additionally, there are significant infrastructure gaps. The region currently accounts for less than 1% of the world's colocation data center capacity, and many countries lack sufficient local data centers, relying heavily on foreign cloud services.[10] This dependency raises concerns about data sovereignty and privacy. While countries like Kenya, South Africa, Egypt, and Nigeria have made progress in establishing data centers, challenges such as unreliable energy supply and high internet costs remain persistent obstacles.[11]

Country Case Study:

Data Governance Progress and Evolution in Ghana

Ghana is recognized as one of the leaders in Africa regarding data governance and privacy regulation. The country's commitment to data protection is anchored in Article 18(2) of the 1992 Constitution of the Fourth Republic of Ghana, which enshrines the right to privacy for its citizens. Before the passage of a dedicated data protection law, Ghanaians largely relied on broader regulations, such as the Electronic Transactions Act of 2008, to safeguard personal data.

In 2012, Ghana took a major step forward by enacting the Data Protection Act (Act 843), a landmark piece of legislation that established clear legal standards for data privacy and protection. Influenced by both regional and international frameworks, this Act laid down the rules for the responsible handling of personal data. Key provisions of Act 843 include: the Establishment of the Data Protection Commission, Rights of Data Subjects, Obligations of Data Controllers and Processors, Data Transfer Restrictions as well as Data Registration Requirements.

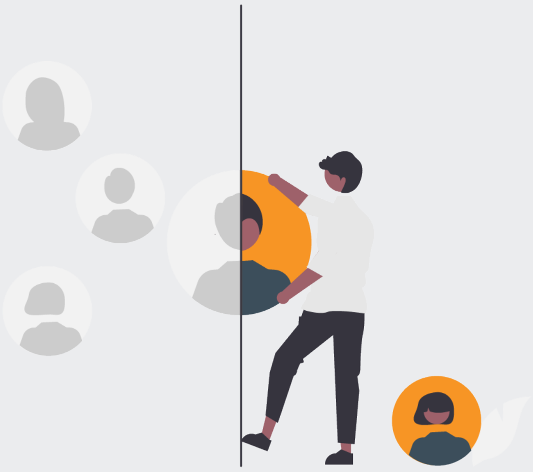
Following the enactment of the Data Protection Act, Ghana has continued to enhance its legal framework with additional laws such as the National Identification Register (Amended) Act, 2017 (Act 750), which supports the implementation of a national ID system, and the Cybersecurity Act, 2020 (Act 1030), which focuses on securing digital systems and protecting data from cyber threats. Additionally, Ghana has a National Data Governance Strategy aimed at creating a robust infrastructure for data management. This strategy seeks to facilitate access to public data, develop mechanisms to build trust between the public and private sectors, and build capacity among individuals and institutions to manage and protect data effectively.

Have Data Protection Laws Been Effective at Protecting Digital Rights and User Safety?

Many data protection laws in Africa were designed to safeguard user data and digital rights but have not been effective at doing this due to enforcement challenges. Some of the specific areas they fall short include:

Limited Public Awareness and Engagement: Governments and Data Protection Authorities (DPAs) often fail to communicate the existence and purpose of these laws effectively. While some governments have attempted to raise awareness, such as Kenya's DPA's attempt to raise awareness through public consultations and media campaigns,[12] their reach has been limited, and many others do not even have assigned DPAs or do not have the budget and resources to do this. Thus, many citizens are unaware and lack understanding of their rights, which limits their ability to hold the government and organizations accountable.

Judicial Interpretation Inconsistencies: In some countries, courts have occasionally struggled to interpret the provisions of Data Protection laws. For example, In a case in Nigeria, that involved a government-owned app that uses tracking technologies and shares data with advertisers without a privacy notice, the court ruled in favor of the government, citing the app's public benefit as outweighing individual privacy rights.[13] This precedent reflects broader judicial challenges in balancing privacy rights with public interest, resulting in inconsistent enforcement and inadequate legal protections for digital rights.



Harmful Exemptions in Laws: Many data protection laws include broad exemptions that undermine their protective scope. These exemptions are often justified on the grounds of national security or legitimate interest, benefiting state agencies at the expense of user rights.[14] Kenya's Data Protection Act includes exemptions for national security, journalism, and research, which can be exploited by malicious actors. Similarly, Uganda's Data Protection and Privacy Act allows data collection from third parties without consent in certain cases, effectively nullifying the same rights these laws are meant to protect.[15]

Cybersecurity Gaps and Data Breaches: Few laws provide explicit guidelines for securing data against emerging threats such as ransomware or advanced persistent threats. Recent incidents such as the Worldcoin biometric data breach.[16] In Kenya, and the Experian data breach in South Africa underscore the region's broader data security challenges.[17] The 2017 Africa cybersecurity report estimates that African economies lost over $3.5 billion to cyberattacks, illustrating the economic and security risks of inadequate data protection.

Underdeveloped Ethical and Governance Frameworks: Laws often fail to address broader ethical issues such as data justice, algorithmic bias, and surveillance. In some cases, governments are the perpetrators, further eroding trust in them as enforcers of these laws. There have been allegations of state-perpetrated surveillance in Uganda with support from Huawei,[18] and also allegations of military-driven digital surveillance in Zimbabwe.[19] Weak regulatory independence and funding exacerbate the issue, as seen in Ghana's Data Protection Commission's silence on privacy risks associated with the Ghana Card.[20]

Data Governance, Artificial Intelligence, and User Safety

Artificial Intelligence (AI) is rapidly advancing, particularly with the rise of generative AI but while it holds a lot of promise and potential to drive innovation, it also comes with a lot of risks which if left unchecked, could have several negative consequences. In Africa, AI's impact is becoming more evident. The 2024 Stanford AI Index ranks Kenya third globally in daily ChatGPT usage, with 27% of Kenyans using the tool regularly, following India and Pakistan.[21][22] This surge has fueled AI-focused startups, research labs, and policy discussions across the continent. Universities in Ghana, Uganda, and South Africa have AI research labs, while companies like Microsoft, Google, and IBM have set up AI hubs in Kenya, Ghana, and South Africa. Mobile banking platforms like M-Pesa use AI for credit scoring.[23] However, ethical concerns persist, such as the use of synthetic media in Rwanda's 2024 elections,[24] deepfakes in Nigeria[25] and Kenya,[26] AI-driven disinformation bots in Ghana.[27] Additionally, the use of AI for surveillance is on the rise in some African countries.[28]

Despite the increasing adoption of AI, regulatory frameworks across Africa remain underdeveloped. AI governance is intrinsically linked to data governance, as AI systems are often trained on large datasets. Currently, no African country has formal AI-focused laws, and only about seven have national AI strategies.[29] At the regional level, the AU has a draft policy that offers guidelines for national regulations.[30] To ensure that AI contributes positively to societal development, it is essential to prioritize user safety, ethical AI use, and robust governance. Policymakers should focus on adapting data governance regulations to include AI, developing principle-based AI policy frameworks, engaging diverse stakeholders, and increasing public awareness to understand the potential risks of AI.

Policy Recommendations

Invest in Public Awareness and Capacity Building

Low public awareness renders even the most comprehensive laws ineffective. Low digital literacy, especially in rural and marginalized communities, also limits the public's understanding of their rights and ability to hold stakeholders accountable. Thus, governments must invest in public education campaigns to demystify these laws and explain how they protect personal data, using simplified, culturally relevant content and local languages. Digital literacy programs should be integrated into national education systems and community outreach initiatives, with tailored content to address different demographics, including rural populations and marginalized communities. Expanding such efforts and collaborating with civil society and the media can empower citizens to recognize breaches, demand accountability, and exercise their rights. Building the technical capacity of relevant stakeholders such as prosecutors, judges, civil society, etc. is also key for proper understanding and enforcement of the law. Governments must adequately fund DPAs, hire skilled personnel, and ensure their independence to effectively hold both public and private entities accountable. Regular training is necessary to address emerging technologies and evolving threats.

Address Harmful Exemptions and Prioritize User Safety

Exemptions in data protection laws, often justified on grounds of national security or public interest, can be exploited to undermine privacy rights. Governments should review and revise data protection laws to narrow the scope of exemptions and ensure that they are applied transparently. Establish oversight mechanisms to monitor the use of exemptions and prevent abuse. Also, enforcement authorities, including the Judiciary should adopt a user-centric approach to enforcement, ensuring that user safety and rights are upheld in the interpretation and enforcement of the law. Additionally, Governments should establish comprehensive cybersecurity frameworks with mandatory security measures, regular security audits, and incident reporting requirements. These frameworks should also address emerging threats such as ransomware attacks and advanced persistent threats to protect personal data from unauthorized access, breaches, and other forms of exploitation.

Invest in Digital Infrastructure to Support Data Governance

Robust digital infrastructure is essential for effective data governance. Governments must invest in secure data storage facilities, reliable broadband access, and advanced cybersecurity technology and infrastructure to ensure the secure collection, processing, and storage of data in compliance with legal standards. It is important to develop national strategies to build and upgrade digital infrastructure, including the establishment of secure data centers and the deployment of nationwide broadband networks. These investments will not only enhance data security but also support broader digital transformation initiatives across sectors.

Conclusion

In summary, the evolution of data governance in Africa, particularly in the context of digital rights, user safety, and emerging technologies like Artificial Intelligence (AI), reflects both progress and significant challenges. While many African countries have enacted data protection laws, their effectiveness is hindered by gaps in public awareness, weak enforcement, and limited judicial expertise. The rise of AI and data-driven technologies amplifies these issues, underscoring the need for adaptive policies that prioritize safety, promote digital literacy, and ensure consistent enforcement. As the digital economy expands, investments in infrastructure, enforcement capacity, and cybersecurity are vital to protect user data and foster trust in digital systems. Governments must address these gaps by developing clear guidelines, strengthening enforcement authorities, and creating adaptable legal frameworks. Such efforts are essential to protecting individual rights, encouraging innovation, and driving sustainable economic growth across the continent.

Appendix

Case Study:

WorldCoin Privacy Violation in Kenya

Worldcoin, a cryptocurrency project co-founded by OpenAI's Sam Altman, encountered significant regulatory and privacy concerns in Kenya following its launch in July 2023. The project incentivized participants to provide biometric data, specifically iris scans, in exchange for 25 WLD tokens (valued at $60). Over 300,000 Kenyans signed up within the first week, raising concerns about privacy, data security, and the potential misuse of sensitive biometric information.[31]

In August 2023, the Kenyan government suspended Worldcoin's activities. Authorities questioned unclear data storage practices and whether participants were adequately informed about the implications of sharing their biometric data. Following a review, the investigation closed in June 2024 without charges and Worldcoin resumed operations.[32] This case underscores significant gaps in Kenya's data governance framework, particularly in regulating emerging technologies like blockchain and biometric data collection. While the suspension and investigation highlighted the government's willingness to address privacy concerns,critics argue that the incident reflects broader issues in public awareness and understanding of digital rights, as well as the capacity of regulatory authorities to enforce data protection laws effectively.

References

1. How much data is generated each day? | World Economic Forum. The World Economic Forum,https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/

2. Digital Transformation Drives Development in Africa. (2024, January 18). World Bank. https://www.worldbank.org/en/results/2024/01/18/digital-transformation-drives-development-in-afe-afw-africa

3. UNDP. (2017, May 15). The Africa Data Revolution Report 2016. https://www.undp.org/africa/publications/africa-data-revolution-report-2016

4. Impact of Mobile Money in SSA. (2024, April 17). World Bank. https://www.worldbank.org/en/publication/globalfindex/brief/data-from-the-global-findex-2021-the-impact-of-mobile-money-in-sub-saharan-africa

5. ICT works. (2024, January 24). 10 Examples of Successful African e-Government Digital Services. https://www.ictworks.org/examples-african-e-government-digital-services/

6. SSA: Report expects smartphone adoption to grow to 87% in 2030. (2023, March 2). Ecofin Agency. https://www.ecofinagency.com/telecom/0203-44312-ssa-report-expects-smartphone-adoption-to-grow-to-87-in-2030

7. Tech Hive Advisory. (2023, December). Roundup on Data Protection in Africa

8.ALT Advisory. (2023, June 28). How independent are African data protection authorities? https://dataprotection.africa/standing-alone-the-independence-of-african-data-protection-authorities/

9. Adequacy. (n.d.). ICO. https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/adequacy/

10. D4D Hub. (n.d.). Data Governance in Africa. https://d4dhub.eu/initiatives/data-governance-in-africa

11. Intelligent CIO. (2024, October 20). Opportunities and challenges in scaling data centres across Africa. https://www.intelligentcio.com/africa/2024/10/20/opportunities-and-challenges-in-scaling-data-centres-across-africa/#:~:text=Despite%20recent%20investments%20in%20data,is%20often%20the%20expensive%20norm.

12. Lawyers hub. (2023, January). Africa Privacy Report 2023/2024.

13. Tech Hive Advisory. (2023, December). Roundup on Data Protection in Africa

14. Access Now. (2024, January). Strengthening Data Protection In Africa: Key Issues For Implementation.

15. IAPP. (2024, February 1). Report examines state of African nations' data protection laws, implementation efforts. https://iapp.org/news/a/evaluating-african-nations-comprehensive-privacy-laws-and-their-implementation/.

16. Ajibade, A. (2024, June 21). Worldcoin to resume operations as police drop investigation in Kenya. Techpoint Africa.https://techpoint.africa/2024/06/21/worldcoin-resume-operations-kenya/

17. The Register & Corfield, G. (2020, September 14). Personal data from Experian on 40% of South Africa's population has been bundled onto a file-sharing website. https://www.theregister.com/2020/09/14/south_africa_experian_data_breach_wesendit/.

18. CNBC. (2019, August 14). Huawei employees intercepted encrypted messages to help African governments spy on political opponents, says WSJ. https://www.cnbc.com/2019/08/14/huawei-employees-helped-african-governments-spy-on-opponents-wsj.html.

19. Munoriyawa, A. (2021, May). The growth of military-driven surveillance in post-2000 Zimbabwe.

20. Graphic Online. (2023, May 5). Stolen identity! Many at risk from SIM card re-registration. https://www.graphic.com.gh/news/general-news/stolen-identity-many-at-risk-from-sim-card-re-registration.html.

21. How AI is impacting policy processes and outcomes in Africa. (2024, May 16). Brookings Institution. https://www.brookings.edu/articles/how-ai-is-impacting-policy-processes-and-outcomes-in-africa/

22. AI Index Report 2024 – Artificial Intelligence Index. (n.d.). AI Index. Retrieved December 16, 2024, from https://aiindex.stanford.edu/report/

23.The Africa Report. (2021, July 20). Will AI risk analysis really expand access to credit in Africa? https://www.theafricareport.com/107432/will-ai-risk-analysis-really-expand-access-to-credit-in-africa/.

24. Thraets. (2024, July 18). https://thraets.org/synthetic-media-in-rwandas-2024-elections/.

25. Anjorin, P. (2022, November 23). How popular Twitter, Facebook accounts shared deepfakes to campaign for Nigerian presidential candidate. Dubawa. Retrieved December 16, 2024, from https://dubawa.org/how-popular-twitter-facebook-accounts-shared-deepfakes-to-campaign-for-nigerian-presidential-candidate/

26. The East African. (2022, August 6). Kenya election: Deep fakes, propaganda, libel inundate social media. https://www.theeastafrican.co.ke/tea/news/east-africa/kenya-election-deep-fakes-propaganda-inundate-social-media-3904934.

27. Haskins, C., Beck, J., & Perlmutter, L. (2024, November 12). AI-powered bots on X spread disinformation in Ghana's election. Rest of World. https://restofworld.org/2024/ghana-election-ai-bots-x-twitter/

28. Institute of Development Studies. (2023, September 27). Mapping the Supply of Surveillance Technologies to Africa: Case Studies from Nigeria, Ghana, Morocco, Malawi, and Zambia. https://www.ids.ac.uk/publications/mapping-the-supply-of-surveillance-technologies-to-africa-case-studies-from-nigeria-ghana-morocco-malawi-and-zambia/

29.Okolo, C. T., & Tano, M. (n.d.). Reforming data regulation to advance AI governance in Africa. Brookings Institution. https://www.brookings.edu/articles/reforming-data-regulation-to-advance-ai-governance-in-africa/

30.Omotosho, B. S. (2024, August 9). Continental Artificial Intelligence Strategy. African Union. https://au.int/en/documents/20240809/continental-artificial-intelligence-strategy

31. The East African. (2023, August 2). Data privacy fears forces Kenya government to suspend World Coin. https://www.theeastafrican.co.ke/tea/sustainability/how-safe-is-sensitive-data-collected-by-worldcoin-4323838

32. Ajibade, A. (2024, June 21). Worldcoin to resume operations as police drop investigation in Kenya. Techpoint Africa.https://techpoint.africa/2024/06/21/worldcoin-resume-operations-kenya/