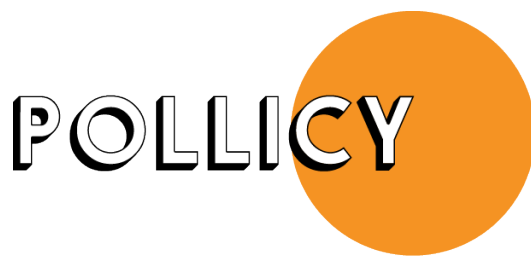


Collective Data Protection

Recommendations for Effective Digital Rights in the Age of AI

AFRICA DATA GOVERNANCE HUB



Collective Data Protection: Recommendations for Effective Digital Rights in the Age of AI

Authors: **Vicente Arias González**, Senior Projects Advisor, Global Solutions Initiative;
Mateo Rodríguez, Assistant to the CEO & Strategic Outreach Manager, Global Solutions Initiative;
Vidisha Mishra, Director, Global Outreach & Policy, Global Solutions Initiative.

Introduction

The growing focus on data governance across Africa marks a positive step toward safeguarding the [digital rights](#)¹ of African citizens (Citizens). However, legislations fail to address novel challenges artificial intelligence (AI) poses to protecting personal data. African states should promote collective association and negotiation mechanisms between Citizens with similar interests and online service providers, nationally and regionally. This approach can empower Citizens to play an active role in determining how personal data about them is collected, used, shared, and managed (processed). This policy brief outlines practical strategies to help Citizens gain meaningful control over the processing of personal data and the conditions under which it occurs.

The Puzzle

Data is critical for developing, training, and effectively operating AI. However, the normative interplay between digital and AI governance fails to substantively address data protection challenges. Current efforts rely too heavily on high-level principles and national legislative frameworks, often disconnected from private organisations' operational realities or the local realities of emerging economies.

The Limitations of High-Level AI Principles

Current international and multilateral AI governance frameworks—such as those from [UNESCO](#), the [European Union](#) (EU), [G20](#), [OECD](#) and the [African Union](#) (AU)—primarily rely on high-level principles to provide Citizens with baseline rights against the risks of AI misuse. Very recently, The [UN Global Digital Compact](#) and the [G20 Rio de Janeiro Leaders' Declaration](#) also highlighted the key role that human rights, privacy, and data protection play in effective AI governance. Most AI principles were enshrined in international frameworks well before the AI boom ([OECD, 2019](#), [G20, 2019](#)).

Consistent international frameworks are essential to AI governance, fostering active collaboration between countries, organisations, and stakeholders to address global and complex AI risks. However, the lack of enforcement mechanisms for these frameworks is an inherent weakness of multilateralism and international law ([Roberts et al., 2024](#)). In the case of AI, this deficiency is compounded by the gap between unenforceable principles and technological practice ([Nabil, 2024](#)).

Moreover, while establishing ethical principles and governance frameworks is important, these efforts alone are often insufficient. They focus on establishing universally applicable principles but offer minimal context-specific recommendations, and fail to address the deeper normative and political conflicts embedded in key concepts like privacy, transparency, and accountability ([Mittelstadt, 2019](#)).

To address such shortcomings, international frameworks rely almost exclusively on national data protection and privacy legislation to safeguard digital rights by protecting personal data in AI-related data processing. The [AU's Continental AI strategy](#), the AU [Digital Compact](#), and the [G20 Maceió Ministerial Declaration on Digital Inclusion for All](#) directly refer to local data protection and privacy laws to protect digital rights against AI-related harms. National AI strategies have also followed this trend, including those in [Rwanda](#), [Benin](#), [Egypt](#), [Mauritius](#), [Senegal](#), [Ghana](#), [Nigeria](#), [Benin](#), and [Uganda](#).

¹ When we say digital rights, we refer to the [African Digital Rights Network's definition](#): “existing human rights but in digital spaces, for example the right to freedom of opinion and expression online, the right to privacy of communication or correspondence when using email or social media, and the right to equitable participation in the social, economic, and political life of the community online”

The Brussels Effect on African Data Laws

The principle-based approach of international frameworks and national AI strategies is complemented by the influence of how the EU, as a digital empire ([Bradford, 2023](#)), addresses digital governance. Although the U.S. and China also exert influence, the EU remains the primary standard setter of digital regulation.

The alignment of African national AI strategies is further explained by the Brussels Effect ([Boshe and Goberna Caride, 2024](#)), the phenomenon whereby regulations established by the EU become global standards, influencing non-EU countries and companies to adopt similar rules.

Since the EU adopted the General Data Protection Regulation (GDPR), over 20 African countries have enacted or are in the process of drafting data protection laws that closely align with its framework ([World Bank, 2024](#)). Regional academic experts have also emphasised harmonising national data protection regulations with international standards like the GDPR ([Shao, 2024](#)). Very few have criticised this process of legal transplantation ([Boshe, 2022](#)).

For example, until adopting its Personal Data Protection regulation, [Ethiopia](#) relied on fragmented, sector-specific rules to govern data processing practices. The new law now closely mirrors the GDPR. Similar cases can be found in [South Africa](#) and [Mauritius](#). [Uganda's](#) data protection regulation was updated to include “[legitimate interest](#)” as a lawful basis for data processing—a central concept in the GDPR. Finally, [Namibia's Data Protection Bill](#), though still in its early stages, has been heavily influenced by the EU framework.

Challenges in Enforcing Digital Rights

International frameworks and the Brussels Effect alone cannot fully address challenges posed to Citizens' digital rights by AI, particularly generative AI. While they provide basic guidelines, imported approaches may overlook local realities and cultural contexts.

As highlighted above, African data protection frameworks struggle to meet the demands of AI development, deployment, and adoption. National regulations cannot often ensure Citizens have a meaningful voice or control over how personal data is processed for training and deploying AI tools. Individualistic and granular approaches to data processing negotiations need significant evolution to address AI's unique challenges effectively.

A core failure of existing data governance lies in consumers' inability to identify who processes data about them or leverage enough market power to enforce their preferences. This imbalance perpetuates unchecked data-sharing practices, enabling third parties with little or no direct relationship with consumers—such as financial institutions, healthcare providers, e-commerce companies, and AI technology firms—to process personal data about Citizens without proper transparency and accountability.

These systemic issues are deeply ingrained in Silicon Valley's business models. A recent interview highlighted this, with former Google CEO Eric Schmidt suggesting that if TikTok were banned in the United States, students should [steal](#) all the platform's data, use LLMs to recreate the program, re-launch it under a new name, and simply hire a team of lawyers to handle the legal aftermath.

In many cases, these practices lead to flagrant breaches of privacy. For example, small unauthorised websites in Nigeria sell Citizens' sensitive personal and financial data for as little as [100 Naira](#) (0,06 USD). Similarly, many lending apps [indiscriminately access sensitive information](#) from Nigerian users without their knowledge or consent.

The South African Artificial Intelligence Association has also called on the country's Information Regulator to investigate LinkedIn for using South African user data to train its AI models [without obtaining consent](#). This concern is not isolated—other major tech companies, including [Nvidia](#), [Anthropic](#), [Apple](#), and [TikTok](#), have been criticised for processing personal data to train generative AI models, often without transparent or ethical practices in place.

Policy Recommendations

To address the regulatory gaps emerging in national data protection legislation due to the rise of AI and building on suggestions encapsulated in [Brazil's T20 2024 Communiqué](#), we recommend a phased approach that [African](#) countries [empower Citizens](#) with greater control over personal data:

Short-Term Actions:

- Recognise collective digital representation rights for Citizens at national and regional levels. For instance, the [Citizens' Bureau in Togo already allows Citizens to refer matters](#) to local elected representatives on issues that concern them.
- Establish collective negotiation organisations, prioritising collaboration between countries with similar data protection legislation.
- Implement these initiatives through executive directives or by extending existing data protection laws to include collective rights.
- Leverage regional bodies like the AU and sub-regional organisations (e.g., ECOWAS, SADC, EAC) to adopt frameworks for mutual recognition of representation rights and collective negotiation.

Mid-Term Actions:

- Represent more African voices in developing governance norms to ensure transparency and accountability for organisations representing Citizens at the global level.
- To design frameworks for collective Citizen representation, draw on use cases from sectors such as finance, pensions, healthcare, and trade unions. For example, [South Africa's Labour Relations Act](#) supports trade unions and collective bargaining, a model adaptable to data processing negotiations.
- Engage data privacy officers and data protection authorities to lead efforts to embed human-centred governance norms.
- Foster a multistakeholder process that includes input from Citizens, governments, and industry players, including the participation of leading AI companies, to build shared frameworks for Citizen representation.

Long-Term Actions:

- Enact legislative reforms to enshrine collective representation and negotiation rights in national laws.
- Amend data protection legislation to define the legal status, funding and responsibilities of organisations representing Citizens' digital rights.
- Countries and multi-regional organisations should endorse adopting emerging technologies that enhance human oversight, transparency and accountability, including Digital Public Infrastructure, throughout the AI lifecycle.

Conclusion

We call on national leaders, industry stakeholders, and civil society organisations to unite and prioritise the inclusion of collective digital rights protection in AI policy frameworks.

Bridging the gap between AI development and safeguarding digital rights is a global challenge, yet Africa is uniquely positioned to lead in this effort. African countries already play a crucial role in leading early production phases in the global [AI supply chain](#). These efforts can be supported by adopting a phased policy approach rooted in regional cooperation, collective representation, and strong oversight; African nations can empower Citizens to have meaningful control over how personal data is handled.

These reforms will tackle urgent issues and position Africa as a global leader in inclusive, human-centred AI governance. At the heart of this mission must be a commitment to transparency, accountability, skills development and Citizen empowerment, ensuring digital rights protection in the evolving AI landscape.

Bibliography

Adams, Rachel. 2022. "AI in Africa: Key Concerns and Policy Considerations for the Future of the Continent." APRI. 2022. <https://afripoli.org/ai-in-africa-key-concerns-and-policy-considerations-for-the-future-of-the-continent>.

"AI Principles." 2019. OECD. 2019. <https://www.oecd.org/en/topics/ai-principles.html>.

Benamara, Akim. 2024. "Nigerian Data Privacy Crisis: Citizens' Personal Information Sold for 100 Naira." TechAfrica News (blog). 2024. <https://techafricanews.com/2024/06/24/nigerian-data-privacy-crisis-citizens-personal-information-sold-for-100-naira/>.

Boshe, Patricia, and Carolina Goberna Caride. 2024. "Is the Brussels Effect Creating a New Legal Order in Africa and Latin America and the Caribbean?" *Technology and Regulation 2024* (March):12–18. <https://doi.org/10.26116/tecchreg.2024.002>.

Boshe, Patricia, Moritz Hennemann, and Ricarda von Meding. 2022. "African Data Protection Laws – Current Regulatory Approaches, Policy Initiatives, and the Way Forward." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network. <https://papers.ssrn.com/abstract=3947664>.

Bradford, Anu. 2023. *Digital Empires: The Global Battle to Regulate Technology*. Oxford University Press.

Cole, Samantha. 2024. "Leaked Documents Show Nvidia Scraping 'A Human Lifetime' of Videos Per Day to Train AI." 404 Media. 2024. <https://www.404media.co/nvidia-ai-scraping-foundational-model-cosmos-project/>.

"Continental Artificial Intelligence Strategy." 2024. African Union. https://au.int/sites/default/files/documents/44004-doc-EN-_Continental_AI_Strategy_July_2024.pdf.

"Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law." 2024. Council of Europe. <https://rm.coe.int/1680afae3c>.

"Data Protection Act." 2017. Government Gazette of Mauritius. https://dataprotection.govmu.org/Documents/DPA_2017_updated.pdf?csf=1&e=0rlrff.

"Data Protection and Privacy Act 2019." 2019. The Uganda Gazette. <https://www.nita.go.ug/laws-regulations/data-protection-and-privacy-act-2019>.

"Digital Compact." 2024. African Union. https://au.int/sites/default/files/documents/44005-doc-AU_Digital_Compact_V4.pdf.

"Draft Data Protection Bill." 2022. Parliament of the Republic of Namibia. https://dataprotection.africa/wp-content/uploads/2022/09/Namibia_DPA-Bill.pdf.

"Egypt's National AI Strategy." 2021. Egypt National Council for Artificial Intelligence. https://mcit.gov.eg/Upcont/Documents/Publications_672021000_Egypt-National-AI-Strategy-English.pdf.

Financial Times. 2024. "Transcript: China's Race to Tech Supremacy — Embracing Africa," May 28, 2024, sec. Transcript. <https://www.ft.com/content/2fa85f2f-255d-49f9-99ac-1e81571d001d>.

Financial Wise, dir. 2024. Eric Schmidt Full Controversial Interview on AI Revolution (Former Google CEO). <https://www.youtube.com/watch?v=mKVFNg3DEng>.

FP Staff. 2024. "TikTok's Parent Co ByteDance Launched New Web Scraper, 'steals' Data from the Web 25X Faster than OpenAI." Firstpost. 2024. <https://www.firstpost.com/tech/tiktoks-parent-co-bytedance-launched-new-web-scraper-steals-data-from-the-web-25x-faster-than-openai-13822040.html>.

"G20 Ministerial Statement on Trade and Digital Economy." 2019. <https://www.mofa.go.jp/files/000486596.pdf>.

"G20 Rio de Janeiro Leaders' Declaration." 2024. G20. https://ec.europa.eu/commission/presscorner/detail/en/statement_24_5941.

Gilbertson, Annie, and Alex Reisner. 2024. "Apple, Nvidia, Anthropic Used Thousands of Swiped YouTube Videos to Train AI." Proof. 2024. <https://www.proofnews.org/apple-nvidia-anthropic-used-thousands-of-swiped-youtube-videos-to-train-ai/>.

"Kazan Declaration: Strengthening Multilateralism for Just Global Development and Security." 2024. BRICS. https://cdn.brics-russia2024.ru/upload/docs/Kazan_Declaration_FINAL.pdf.

"Labour Relations Act 66 of 1995." 1995. South African Office of the President. https://www.gov.za/sites/default/files/gcis_document/201409/act66-1995labourrelations.pdf.

"Maceió Ministerial Declaration on Digital Inclusion for All." 2024. G20. https://southsouthpoint.net/wp-content/uploads/2024/09/G20_Maceio_Ministerial_Declaration_2024_1726361028.pdf.

"Mauritius Artificial Intelligence Strategy." 2018. Working Group on Artificial Intelligence. <https://ncb.govmu.org/ncb/strategicplans/MauritiusAIStrategy2018.pdf>.

Metodjo, Alain. 2024. "Citizen Network: Citizen Participation in Africa." Citizen Network. 2024. <https://citizen-network.org/library/citizen-participation-in-africa.html>.

Mittelstadt, Brent. 2019. "Principles Alone Cannot Guarantee Ethical AI." SSRN Electronic Journal. <https://doi.org/10.2139/ssrn.3391293>.

Nabil, Ryan. 2024. "Global AI Governance and the United Nations." Yale Journal of International Affairs. February 2, 2024. <https://www.yalejournal.org/publications/global-ai-governance-and-the-united-nations>.

"National Strategy Ghana." 2023. AI Policy Lab by LawyersHub. 2023. <https://www.aipolicy.africa/national-strategies/32da1df4-973e-49c8-95fa-ab41c132515c>.

"National Strategy Nigeria." 2024. AI Policy Lab by LawyersHub. 2024. <https://www.aipolicy.africa/national-strategies/56d0e2c4-a1c1-44b6-807d-80905955068b>.

"National AI Policy." 2022. The Republic of Rwanda - Ministry of ICT and Innovation. https://rura.rw/fileadmin/Documents/ICT/Laws/Rwanda_national_Artificial_intelligence_Policy.pdf.

"National Artificial Intelligence and Big Data Strategy." 2023. Benin's Ministry of Digital and Digitalization. <https://numerique.gouv.bj/assets/documents/national-artificial-intelligence-and-big>

data-strategy-1682673348.pdf.

“National Strategy Benin.” 2023. AI Policy Lab by LawyersHub. 2023. <https://www.aipolicy.africa/national-strategies/0e574345-6d15-4eb3-b6b2-b2f039b2db48>.

“National Strategy Uganda.” 2023. AI Policy Lab by LawyersHub. 2023. <https://www.aipolicy.africa/national-strategies/1cb428e6-49e4-45d3-bc92-bb411ac7b3ed>.

“Proclamation to Provide for Personal Data Protection.” 2024. Federal Negarit Gazette of the Federal Democratic Republic of Ethiopia. https://www.dataguidance.com/sites/default/files/personal_data_protection_proclamation_1321-2024.pdf.

“Protection of Personal Information Act (PoPIA).” 2013. Parliament of South Africa. <https://popia.co.za/section-11-consent-justification-and-objection/>.

“Recommendation on the Ethics of Artificial Intelligence - UNESCO Digital Library.” 2021. UNESCO. 2021. <https://unesdoc.unesco.org/ark:/48223/pf0000381137>.

“Regulating Digital Data in Africa.” 2023. World Bank. <https://documents1.worldbank.org/curated/en/099051924164028010/pdf/P1724171504d3f03e19f251b7aa4316bb23.pdf>.

Roberts, Huw, Emmie Hine, Mariarosaria Taddeo, and Luciano Floridi. 2024. “Global AI Governance: Barriers and Pathways Forward.” *International Affairs* 100 (3): 1275–86. <https://doi.org/10.1093/ia/iae073>.

Schutters, Lindsey. 2024. “Local Industry Watchdog Sounds Alarm over AI Stealing South African Data on LinkedIn.” 2024. <https://www.zawya.com/en/world/africa/local-industry-watchdog-sounds-alarm-over-ai-stealing-south-african-data-on-linkedin-x1td8rer>.

Shao, Deo, Fredrick Ishengoma, Anastasija Nikiforova, and Mrisho Swetu. 2024. “Comparative Analysis of Data Protection Regulations in East African Countries.” *Digital Policy, Regulation and Governance* ahead-of-print (ahead-of-print). <https://doi.org/10.1108/DPRG-06-2024-0120>.

Snowder, Dennis, and Paul Twomey. 2022. “Empowering Digital Citizens: Making Humane Markets Work in the Digital Age.” *The Global Initiative for Digital Empowerment*. <https://thegide.org/wp-content/uploads/2022/11/GIDE-report-final-version.pdf>.

“Stratégie Nationale et Feuille de Route Du Sénégal Sur l’Intelligence Artificielle.” 2023. Ministre de la Communication, des Télécommunications et du Numérique. <https://ai4d.ai/wp-content/uploads/2023/10/reesumee-strategie-nationale-ia-senegal.pdf>.

“T20 Brasil 2024 Communiqué.” 2024. Think20. <https://t20brasil.org/en/communique>.

“The Data Protection and Privacy Regulations 2021.” 2021. The Uganda Gazette. <https://www.unwantedwitness.org/download/uploads/Uganda-Data-Protection-and-Privacy-Act-2019-Regulations.pdf>.

“What Are Digital Rights?” 2024. 2024. <https://www.africandigitalrightsnetwork.org/what-are-digital-rights->

