

AI in Africa: regional data protection and privacy policy

- ❖ This policy brief examines the institutional challenges of data protection policy cooperation in Africa as emerging AI-driven technological developments grow ahead of institutional, social and cultural changes.
- ❖ The slow pace of data governance policy evolution and processes within the African Union is a major hindrance to a harmonised policy framework for data protection and privacy on the continent.
- ❖ There are significant variations in cultural and legal diversity, technology access, and governance capacity for data-related policy making across Africa, making a harmonised data protection and privacy policy framework for the continent a daunting challenge.
- ❖ The current lack of capacity and technical expertise across the policy-making echelon for data governance in Africa poses a significant implementation and process management cost for a harmonised regional policy framework for the continent.
- ❖ Engagements with and adoption of AI-related data policy in the continent can be driven by matching AI-enabled technology solutions with specific socio-economic needs
- ❖ A regional data protection and privacy policy framework for Africa will catalyse regional collaboration and cooperation in dealing with the emerging issues and risks posed by artificial intelligence deployments on the continent.
- ❖ An African data protection and privacy policy framework needs also to be aligned to and harmonised with other similar instruments globally so as not to impose unnecessary costs and raise unwanted conflicts with other national data protection and privacy regimes.
- ❖ A full-scale critical review of the current state of regional data protection frameworks in Africa is required to improve effectiveness in dealing with emerging the challenges and concerns raised by artificial intelligence systems.
- ❖ However, Africa also needs to learn from other regions that have moved forward earlier with policies and practices relevant to data protection and related cyber-policy, while at the same time focusing on priority contextual concerns, including the related principles of privacy, openness and bias, within a policy framework that balances innovation and data protection

Introduction

With the economic and social role of artificial intelligence (AI) and its prevalence predicted to grow significantly, there seem as yet few collective attempts at either regional or

continental level in Africa aimed at regulating the critical emerging issues presented by AI. This is especially so as regards data protection and privacy, including government surveillance or corporate influence over customers.

It is therefore imperative to initiate critical discussion in respect of AI policy, law and regulation in the region. Such discussion needs to be context-specific, to look at the requirements to adapt existing regulation or formulate new policy. Such an engagement can provide a coherent, regional-level policy roadmap to channel the massive potential of AI deployments on the continent. It can also provide an appropriate institutional configuration for international cooperation on data protection and privacy.

The study undertaken here explores AI-related data protection and privacy governance at both continental (in relation to the African Union) and regional levels (with a focus on ECOWAS), in as countries begin to grapple with AI in a rapidly changing socio-technical environment.

It analyses the evolution, processes and attributes of data governance policy by African regional bodies. It further examines the challenges and opportunities of a multilateral approach to formulating and adopting cyber-policy with respect to data protection and privacy on the continent.

The study approach comprised a comprehensive review and analysis of pertinent cyber-governance literature, with a focus on data protection policy in relation to AI. The aim here was to highlight critical gaps, explore the challenges and opportunities, and generate new thinking on regional and continental-level data governance mechanisms on the continent. The output of the literature analysis was used to design and conduct semi-structured interviews with cyber-governance professionals and policy experts at both the governmental and inter-governmental levels on the continent.

The state of play

Africa needs sound protection and privacy policy frameworks as critical safeguards to maximise the benefits of AI deployments.

Some technology experts are predicting an proliferation of the adoption of AI in Africa similar to the uptake of mobile phones claiming it will help leapfrog development on the continent.¹ In this context, the adoption and effective implementation of sound protection and privacy policy frameworks is a fundamental reference point to ensure that critical safeguards are in place in order to maximise the benefits of AI deployments on the continent. Such frameworks are severely limited at present.

The closest policy document on the continent dealing with these issues is the 2014 *African Union Convention on Cyber Security and Personal Data Protection* (known as the Malabo Convention).² However, support for the Malabo Convention has been slow in coming.

¹ Aleksandra Gadzala. 'Coming to Life: Artificial Intelligence in Africa', Washington DC, Atlantic Council, November 2018, <https://www.atlanticcouncil.org/images/publications/Coming-to-Life-Artificial-Intelligence-in-Africa.pdf>, WEF, 'Revolutionary technologies will drive African prosperity - this is why', Geneva, World Economic Forum, <https://www.weforum.org/agenda/2019/09/why-the-4ir-is-a-fast-track-to-african-prosperity/>.

² AU, 'African Union Convention on Cyber Security and Personal Data Protection,, Addis Ababa, African Union, https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

Africa needs greater coherence between cyber-security and personal data protection instruments at continental, regional and national levels.

Currently only 5 of the AU's 55 member states have fully ratified³ the Convention, whilst a further 14⁴ have signed it.⁵ While the treaty provides "fundamental principles and guidelines to ensure an effective protection of personal data and create a safe digital environment for citizens, security and privacy of individuals' data online",⁶ it makes no reference to institutional strategies for mitigating the threats posed specifically by AI deployments on the continent.

At the sub-regional level, the focus has largely been on the policy element of data privacy. The Economic Community of West African States (ECOWAS) has led the way via the 2010 *Supplementary Act on Personal Data Protection within ECOWAS*⁷. Similar policy instruments have also been developed by the East African Community (EAC) – viz. the 2011 *Bill of Rights*⁸ and the 2008 *Draft EAC Legal Framework for Cyber Laws*⁹ – and by the Southern African Development Community (SADC) – the 2012 *Model Law on Data Protection*¹⁰. However, both are non-binding on member states, making implementation and enforcement difficult.¹¹ Differences in the formulation of the various policies further undermine levels of compliance.

The continent, therefore, requires a greater level coherence for facilitate adoption and implementation. Without this, the gap between the frontiers of global technology policy and the mechanisms of local and regional governance will widen, with geopolitical ramifications for the continent. To help close this gap, research into the challenges of AI-related data protection policy mechanisms, along with the slow adoption of a continental-level data protection framework, is needed in order to offer evidence-based recommendations to address the situation. This in turn will strengthen the efficacy of collective approaches to data protection policy and regulation as it relates to the peculiarities of AI in the African context. This process will help ensure that the transnational benefits of AI deployments, as they emerge on the continent, work for both public and societal good, while minimising risks.

³ Ghana, Guinea, Mauritius, Namibia & Senegal.

⁴ Benin, Chad, Comoros, Congo, Ghana, Guinea-Bissau, Mozambique, Mauritania, Rwanda, Sierra Leone, Sao Tome & Principe, Togo, Tunisia & Zambia.

⁵ Accessed September 21, 2019: <https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf>

⁶ African Union Cyber Security Expert Group Terms of Reference (ToR). https://au.int/sites/default/files/announcements/34877-annc-au_cyber_security_expertgroup_tors.pdf.

⁷ ECOWAS, 'Supplementary Act A1SA.1/01/10 on Personal Data Protection within ECOWAS', 2010, <https://ccdcoe-admin.aku.co/wp-content/uploads/2018/11/ECOWAS-110819-FightingCybercrime.pdf>.

⁸ EAC, 'The East African Community Human and Peoples Rights Bill', East African Community, 2011, http://www.eala.org/uploads/Eac_human_14-Sep-2016_11-11-55-ilovepdf-compressed.pdf.

⁹ EAC, 'Draft EAC Legal Framework for Cyber Laws', East African Community, 2008, <http://repository.eac.int/bitstream/handle/11671/1815/EAC%20Framework%20for%20Cyberlaws.pdf>

¹⁰ SADC, 'Data Protection: Southern African Development Community (SADC) Model Law', Southern African Development Community, 2012, https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL_DOCUMENTS/FINAL_DOCS_ENGLISH/sadc_model_law_data_protection.pdf.

¹¹ Yarik Turianskyi, 'Balancing Cyber Security and Internet Freedom in Africa', AfricaPortal, 2018, <https://www.africaportal.org/publications/balancing-cyber-security-and-Internet-freedom-africa/>.

In this regard, according to one commentator:

*Policymaking and regulation at the level of international union requires a correct balance between the benefits of the harmonisation of policies and the internalisation of cross-country spillovers and the costs related to heterogeneous preferences of the countries that take a decision in common.*¹²

While compliance with regional data protection and privacy policy frameworks is important, it is also necessary to assess their efficacy in dealing with emerging challenges posed by AI deployments. Any changes thus proposed should be adopted in a manner that will not weaken either data protection itself or impede the benefits of AI. This requires a principle-based policy-making process aligned with the contextual nuances of the region.

Artificial intelligence and transnational data governance

The nexus between AI and data is driven by three key change mechanisms: massive computing power; complex algorithms; and big data.

The nexus between AI and data is driven by three key change mechanisms: massive computing power; complex algorithms; and huge volumes of data, both structured and unstructured, derived from a wide range of sources, including search engines and social media activity.¹³ These mechanisms are altering the traditional scope of informed consent and access, control and processing of data, especially with regard to identifiability, opacity and unpredictability of data outcomes. Traditional data protection and privacy policies, therefore, need to be adapted to cater for the realities of AI.¹⁴ Effective regulation for data protection is important, not only for privacy and security, but also to ensure data quality to stimulate innovation.

Transnational data protection policy and governance seeks to regulate data capture and processing as data moves across national boundaries, in order to minimise risks and maximise opportunities. Consequently, international cooperation is required to mitigate the threat of cybersecurity and data breaches, especially as they relate to the application of AI.¹⁵ This makes collaboration between transnational institutions and national regulatory

¹² Alex B. Makulilo, 'Myth and reality of harmonisation of data privacy policies in Africa', *Computer Law & Security Review*, 31(1), 2015.

¹³ Cf: Alex Campolo, Madelyn Sanfilippo, Meredith Whittaker, and Kate Crawford, 'AI Now Report', New York, AI Now Institute, 2017, https://ainowinstitute.org/AI_Now_2017_Report.pdf; OVIC, 'Artificial intelligence and privacy', Melbourne, Office of the Victorian Information Commissioner, 2018, <https://ovic.vic.gov.au/wp-content/uploads/2018/08/AI-Issues-Paper-V1.1.pdf>

¹⁴ Christopher Kuner, Fred H. Cate, Orla Lynskey, Christopher Millard, Nora Ni Loideain, and Dan Jerker B. Svantesson. 'Expanding the artificial intelligence-data protection debate', *International Data Privacy Law*, 8(4), (2018), 289 – 292.

¹⁵ Abraham D. Sofaer and Seymour E. Goodman 'Cyber crime and security. The transnational dimension', Hoover Institution Press, 2001; Tim Maurer. 'Cyber norm emergence at the United Nations', Harvard MA, Belfer Center for Science and International Affairs, 2011); Virginia Greiman 'Reflecting on Cyber Governance for a new World Order: An Ontological Approach', in *ECRM 2018 17th European Conference on Research Methods in Business and Management*. Academic Conferences and Publishing Limited, 2018.

entities more effective as a governance lever to address cyber policy challenges than tackling them in national silos.¹⁶

The ECOWAS Data Protection Convention in context

The 2010 ECOWAS *Supplementary Act on Personal Data Protection*¹⁷ covers critical data protection provisions and exceptions such as data access rights, the declaration of compulsory data processing, sensitive data authorisation as well as guiding principles for personal data processing. However, in contrast to some other regional data protection frameworks - such as the recent European Union *General Data Protection Regulation*¹⁸ (GDPR) and the 2013 OECD privacy guidelines¹⁹ to some extent - key data protection principles with significant imperatives for AI developments are missing. These include those governing: the notification of data security breaches, especially for automated decision-making; data portability; the right not to be subjected to automated decision-making; and the 'right to be forgotten'.²⁰ Some of these limitations that require critical review are summarised in Table 1.

These policy limitations need to be reviewed in the era of AI deployments as machine learning feeds on large datasets from connected devices which may not necessarily have been collected with due transparency. The critical reappraisal of AI-related data protection and privacy policy frameworks needs to be driven by a shift towards a risk-based, use-biased approach to data stewardship and towards empowering data subjects rather than data controllers, especially with respect to issues such as consent. This will help to repurpose the objective of data protection and privacy, from terms of collection to the risks and impacts of processing and usage.

International conventions protect key rights in respect of individuals' data and set out for personal data processing.

¹⁶ Lawrence B. Solum, 'Models of Internet governance.' *Internet governance: infrastructure and institutions*, 2009; David Mussington, Brent J. Arnold, Benoît Dupont, Scott Hilts, Timothy Grayson, Christian Leuprecht, Liam Nevill, Brian O'Higgins, and Josh Tupler. 'Governing Cyber Security in Canada, Australia and the United States.' Ontario, Centre for International Governance Innovation, 2018.

¹⁷ ECOWAS, 'Supplementary Act A1SA.1/01/10 on Personal Data Protection within ECOWAS', 2010, <https://ccdcoc-admin.aku.co/wp-content/uploads/2018/11/ECOWAS-110819-FightingCybercrime.pdf>.

¹⁸ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

¹⁹ OECD, 'Revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data', Organisation for Economic Cooperation and Development, 2013, http://oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

²⁰ Graham Greenleaf, and Bertil Cottier. 'Data Privacy Laws and Bills: Growth in Africa, GDPR Influence', *Privacy Laws & Business International Report*, 2018; OVIC, 'Artificial intelligence and privacy', Melbourne, Office of the Victorian Information Commissioner, 2018, <https://ovic.vic.gov.au/wp-content/uploads/2018/08/AI-Issues-Paper-V1.1.pdf>.

Table 1: ECOWAS Data Protection Act compared to other regional policy frameworks

Principles	ECOWAS (2010)	OECD (2013)	GDPR (2016)
<i>Automated decision-making: Prohibition</i>	Yes	No	No
Automated decision-making: Right to object	No	No	Yes
<i>Automated decision-making: Right to logic information</i>	No	No	Yes
<i>Data controller obligation: Data protection by default</i>	No	No	Yes
<i>Data controller obligation: Data protection by design</i>	No	No	Yes
<i>Data controller obligation: Notification</i>	No	Yes	Yes
<i>Data controller obligation: Risk or impact assessments</i>	No	Yes	Yes
<i>Data subject right: Data portability</i>	No	No	Yes
<i>Data subject right: Right to be forgotten</i>	No	No	Yes
<i>Liability: Data controller and processors</i>	No	No	Yes
<i>Territorial scope: Data has to be processed according to rules of the data subject jurisdiction no matter where the processing is taking place</i>	No	No	Yes
<i>Trans-border data flow: Privacy may not restrict free flow of personal data</i>	No	Yes	Yes
Sources:			

Unprecedented economic growth and the advent of new digital technologies - including AI - bring the issues of online privacy rights and data protection to the fore.

Institutional challenges and cooperation

The unprecedented growth in Africa's digital economy, the advent of the so-called 4th Industrial Revolution, and the expansion of digital technologies such as AI bring the issues of online privacy rights and data protection to the fore. Although Africa's average Internet penetration is a lowly 25%, access has grown dramatically over the past decade.²¹ However, institutional, social and cultural changes have not kept pace. Currently only 23*** out the

²¹www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf

55 member states of the African Union (AU) have comprehensive data protection and privacy legislation in place, although a further 12 are in the process of doing so.

The slow pace of data governance policy evolution across the AU hinders the development of a harmonised policy framework for data protection and privacy.

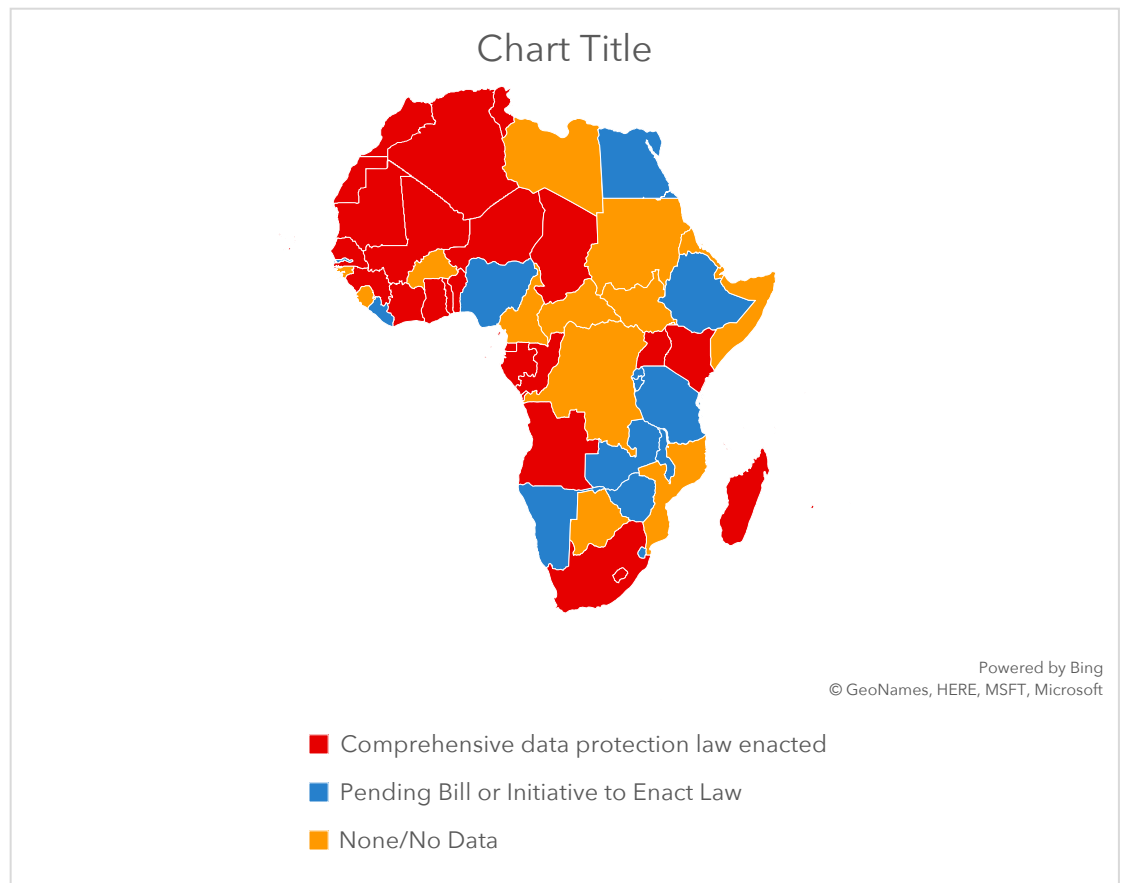
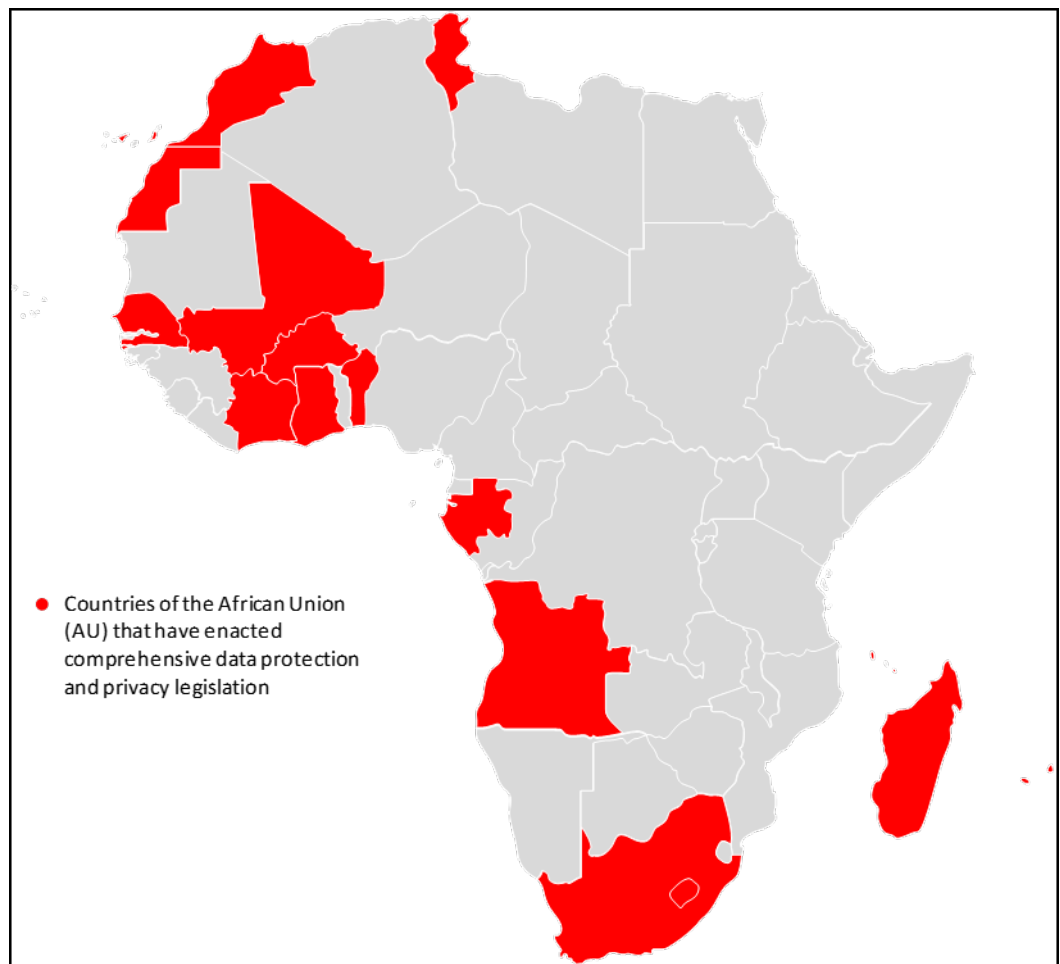


Figure 1: Data protection and privacy legislation landscape in AfricaSource: Banisar²²

This slow pace of data governance policy evolution across the AU member states is a major hindrance to a harmonised policy framework for data protection and privacy within the ambit of AI developments. It is noteworthy that more countries in Africa that have enacted comprehensive data protection and privacy legislation than the number that have adopted the continent's Malabo Convention discussed above. Further, most of the national data protection laws predate the Malabo Convention, and many have more specific provisions for data protection than the AU convention.

In addition, the policy process at continental level is a slow and painstaking process. As result, countries in a hurry to implement data policy issues and privacy measures are moving ahead without necessarily looking to the region for guidance. Further, the largely top-down and poorly-consulted approach to data policy engagement by the AU and the Regional Economic Communities (RECs) creates significant buy-in and adoption challenges. Indeed, some have complained that a top-down regional policy engagement process might

²² Banisar, D, 'National Comprehensive Data Protection/Privacy Laws and Bills 2018', Rochester, NY, Social Science Research Network, August 2019, <https://papers.ssrn.com/abstract=1951416>.

only be designed to “serve narrow regime interests at the expense of broader national and collective interests”²³. Another adoption challenge with the Malabo Convention – like the GDPR – is its lack of sector- or industry-specific considerations with regard to data protection and privacy guidelines. This creates unhelpful levels of uncertainty and unpredictability for multinational bodies seeking compliance within member states.²⁴

Another critical hindrance to data protection and privacy policy cooperation on the continent is caused by significant variations in cultural and legal traditions, differing levels of access to technology, and variations in data-related governance capacity across Africa.²⁵ Further, the policy-making institutions in Africa are largely led by an analogue generation that predates the Internet age, leading to a lack of capacity to understand and engage with data-related digital policy engagement and its imperatives for digital rights. This general lack of understanding leads to a lack of policy direction with respect to AI and its associated emerging issues.

Cross-country spill-over****

On the one hand, an Africa-wide data protection and privacy policy framework will catalyse regional collaboration and cooperation to deal with the emerging issues and risks posed by artificial intelligence deployments. On the other, it may impose costs and raise conflicts with other national data protection and privacy regimes, if it is not well harmonised with global frameworks

The Malabo Convention is, therefore, a good place to start – but the AU will need to do much more work in promoting its basis and benefits, and to address cross-country spill-over. This will demonstrate the benefits of a harmonised data protection and privacy policy framework, rather than highlighting the accruable costs for member states.

Benefits of a harmonized data protection framework

In an increasingly networked society with more open borders, a regionally-harmonised data protection policy would be beneficial for Africa, as member states will be able to negotiate data policy agreements as a regional block. This will mean a stronger capacity to reject unfair terms and to strengthen the regional market as business progressively drives technology adoption. Overall, a clear continental data protection and policy framework will

²³Söderbaum, F, Skansholm, H, & Brolin, T, 'From Top-Down to Flexible Cooperation - Rethinking Regional Support to Africa', Uppsala, Nordic Africa Institute, <http://cris.unu.edu/sites/cris.unu.edu/files/From%20Top%20Down%20to%20Flexible%20Cooperation%20-%20May%202016.pdf>.

²⁴AANOIP, 'The Africa Continental Free Trade Agreement and Cross-Border Data Transfer: Maximising the Trade Deal in the age of Digital Economy', African Academic Network on Internet Policy, 2019, <http://www.aanoip.org/the-africa-continental-free-trade-agreement-and-cross-border-data-transfer-maximising-the-trade-deal-in-the-age-of-digital-economy/>

²⁵Mabika, V, 'The Internet Society and African Union Commission Launch Personal Data Protection Guidelines for Africa', The Internet Society, 2018, <http://www.Internetsociety.org/blog/2018/05/the-Internet-society-and-african-union-commission-launch-personal-data-protections-guidelines-for-africa/>

give member states more capacity to hold to account the large data handling firms, and to ensure responsible behaviour - as the GDPR is doing in Europe.

An Africa-wide data protection and privacy policy framework will catalyse regional collaboration to address the emerging issues and risks posed by artificial intelligence deployments.

Another positive is that a regional framework will enable member states to leverage and learn from each other. Emerging AI data policy issues present African countries with an opportunity to learn from one another in developing data governance policy, both nationally and at continental level. Four African countries are already leading the way in this regard - Cape Verde, Mauritius, Senegal, and Tunisia - having already acceded to the Council of Europe Treaty 'Convention 108'²⁶ for the protection of individuals with regard to the automated processing of personal data. This Convention has been updated to align it with the GDPR, making it the only internationally binding agreement on data protection and privacy in respect of AI. As signatories to Convention 108, these African countries are bound by its new legal framework reinforcing protection for personal data collection and processing. This will help mitigate the data risks of AI systems, along similar lines to EU member states, and serves as an exemplar of how emerging AI-related issues can be addressed with effective data protection interventions.

Capacitating policy-makers

The lack of data governance capacity and technical expertise at the policy-making level in Africa imposes a significant costs of implementation and process management for a harmonised regional policy framework. Further training and assistance for policy makers is required, the more so as many AU member states are yet to establish independent data privacy regulatory authorities. If this policy-making capacity gap to deal with these emerging technological and data policy challenges is not bridged, this will serve to limit the competitiveness of the continent. It is also of key importance for regulating the global enterprises that collect, process and share user data for AI-based applications and services, especially those in the mobile space.

However, a harmonised regional data protection policy regime might impose enforcement costs on African countries that lack the required resources for implementation and enforcement.²⁷ Funding will be necessary to set up data protection authorities (DPAs) at the government level. Private sector players too will need to fund designated data privacy representatives.

²⁶ CoE, 'Convention 108 and Protocols', Brussels: Council of Europe, <https://www.coe.int/en/web/data-protection/convention108-and-protocol>.

²⁷ Tiffany, C, 'Privacy Harmonization and the Developing World: The Impact of the EU's General Data Protection Regulation on Developing Economies', *Wash. JL Tech. & Arts* 12, 2016.

Data protection laws and frameworks are built on general principles, which guide and form the basis of specific measures and interventions.

Principles and values to coordinate AI data protection

Data protection laws and frameworks are built on general principles, like most technology laws. This empowers them to regulate appropriate behaviour within a societal context regardless of technology evolution with time.

Critical among these principles for Africa is the right to privacy of an individual. It is fundamental for our existence as human beings. Protecting the right to privacy will allow innovation and creativity to thrive without intrusive monitoring and surveillance. Once the fundamental principles are properly in place, laws do not have to necessarily change to cater for AI – unless, of course, they embody bad practice or are insufficient to cater for emerging data protection challenges arising from AI.

Furthermore, people need to become more aware with respect to transparency and openness. They need to know that there are built-in safeguards to protect their personal data from being collected for misuse, or for further processing that is incompatible with the purpose for which the data was collected in the first place. These principles remain fundamental in building trust within the technology ecosystem.

Another principal area of concern with AI policy is the issue of bias arising from the disproportionate amount of investment received by the US, China and the EU (over 93% of global private equity investment in AI between 2011 and mid-2018).²⁸ There is limited data being fed into AI algorithms that correlates with the African experience. AI policy must fit the African experience, including catering for marginalised groups, covering the diversity of different languages and cultures across the region, and addressing issues of gender bias, in order to achieve a broad-based African solutions appropriate to African issues.

In addition and in the longer term, a coherent regional data policy framework should be technologically-neutral and consistent across multiple industry sectors and services. Further, risk assessment models should be built into the regional frameworks in such a way as to reflect accepted privacy principles.

Adapting data protection policies for AI

In order to ensure that regional data protection frameworks in Africa are sufficient to deal with the emerging challenges of AI, it is necessary to review them in order to identify and address areas of concern. This will ensure a degree of consistency in terms of the laws adopted across the continent, and allow for greater correspondence between African countries, as well as between Africa and the rest of the world.

In adapting current regional data protection frameworks in Africa to deal effectively with the emerging challenges of AI systems, there needs to be a balance between slavish policy transfer and learn the lessons from other regions that have moved forward earlier with

²⁸ OECD, Private Equity Investment in Artificial Intelligence, 2018, <https://www.oecd.org/going-digital/ai/private-equity-investment-in-artificial-intelligence.pdf>,

policies and practices relevant to data protection and related cyber policy. While the GDPR is a model for regional data protection policy collaboration, it is not a universal panacea, and can be improved upon.

Following on from the GDPR, and considering the cross-border imperatives of AI systems, regional data policy instruments should be framed so as to require data handling firms operating in Africa to sign up to the data protection and privacy laws wherever they are operating whether or not they are registered as a business entity in those jurisdictions. This is of significant importance for Africa, considering the fact that many critical, data-related projects across the continent are handled and processed outside its borders.

AU member states need to collaborate to ensure appropriate institutional arrangements for a harmonised data protection policy to address the emerging issues of AI.

Institutional arrangements for AI data protection

Collaboration across the AU member states in order to ensure as much alignment as possible is imperative to ensure appropriate institutional arrangements for a harmonised data protection policy in Africa that can effectively deal with the emerging issues of AI. Secondly, and perhaps more challenging, is the need to ensure collaboration and partnership across multiple industry sectors: the existing regional data protection framework is too narrow, and needs to be broadened to be applicable across multiple industry sectors.

The cross-border nature of data collection and processing goes beyond the jurisdiction of the IT ministries of member states adequately to address AI-related data protection and privacy. In order, therefore, to guarantee more effective policy implementation, the AU may need to give some independent authority to an appropriate institutional body to be able to deal with the emerging issues across the continent and within member states. The optimal institutional framework requires a more broad-based approach to addressing AI-related data protection and privacy issues on the continent.

Within the context of the international legal framework, however, national laws still have to be adopted and implemented and ratified by the specific countries. Irrespective of a regional framework, member states are the nevertheless the jurisdictions where laws need to be applied. A multi-pronged approach involving both regional and national frameworks is therefore likely to be optimal.

A multi-stakeholder model is also necessary to strengthen the effectiveness of the institutional framework for a harmonised data policy for the region. Multi-stakeholderism can provide the platform for different institutions to work together at the same time within both national and regional policy systems, and offers effective peer review mechanisms at both the country and sub-regional levels. Within this process, governments, citizens, universities, the private sector and civil society should collaborate optimally to enact and adapt regulatory frameworks in such a manner that promotes digital innovation while protecting the privacy and security of citizens.

Conclusion and policy recommendations

A co-regulatory approach, collaboratively driven by the industry, technical and civil society stakeholder groups, is needed to regulate issues arising from AI.

With less than half of AU member states having enacted comprehensive data protection and privacy legislation, with much of the new data protection regimes are new and lacking in capacity, the imperative for a harmonised regional data protection regime for the continent becomes even more significant to ensure personal data protection is not undermined when data flows across borders, especially in the era of AI.

Nevertheless, given the cost constraints of a harmonised regional data protection framework for the continent, a **co-regulatory model** is proposed. This model should be collaboratively driven by the industry, technical and civil society stakeholder groups. It should focus on the development of data protection and privacy standards – drawing on AI-specific stakeholder expertise – in the context of government-led policy and legal guidelines.²⁹ This will make implementation more cost-efficient as appropriate standards are developed by the regulated entities. This will engender commitment, without stifling innovation for social good within the region.

With this model therefore, another framework may not necessarily be the way forward. Regional governments might rather **develop clearer guidelines** based on the existing laws and policies. Such technology-neutral guidelines can assist to operationalise the issues raised by AI, based on agreed fundamental principles, taking into cognisance contextual and sectoral uniqueness. This will make for more practical implementation rather than devising new AI-specific laws. In the case of Europe, some Data Protection Regulators are empowered and authorised to issue guidelines on an ongoing basis to cater for technology developments.

It is not so much a framework that is required, but an **implementation strategy**. This includes equipping regulators with the knowledge and skills to grapple with and address the issues and concerns arising from the deployment of AI. This includes considering the significant cross-border imperatives of AI deployments as well as cross-sectoral technological developments. And it involves capacitating the regional entities in Africa for innovative, evidence-based implementation, with the support and involvement of all industries and all stakeholders.

To address the technology policy capacity gap on the continent, it is recommended that teams of AI experts are brought together to undertake research and establish a **knowledge base**. This could be extended to the establishment of AI knowledge centres across the region to support the design and formulation of policies governing AI. In this regard, some private sector global technology firms like Google and Microsoft are already active in AI on the continent: Google recently launched an artificial intelligence lab Ghana, the first in Africa; and a Master's of Machine Intelligence degree, backed by Facebook and Google, was

²⁹ Tiffany Curtiss, 'Privacy Harmonization and the Developing World: The Impact of the EU's General Data Protection Regulation on Developing Economies', *Washington Journal of Law, Technology & Arts*, Vol 12, 2016.

launched in Rwanda. Similarly, the University of Oxford is supporting the development of regional hubs across the world to support capacity building in a wide range of areas, including AI-related data protection. The AU should get involved with the development of one or more of these regional hubs in Africa.

Finding **AI-enabled solutions** to the socio-economic challenges facing Africa is an important avenue to drive engagement with and adoption of AI-related data policy. A needs analysis of countries need with respect to AI technology solutions will assist in matching policy with economic solutions.

At the continental level, there should be more **engagement between member states** in the development of data policies in order to ensure higher levels of adoption afterwards.

For more RIA updates, sign up [here](#) and download full South Africa report [Hyperlink](#)

Author

Raymond Onuoha: ronuoha@lbs.edu.ng

Enquiries

info@researchictafrica.net

409 The Studios, Old Castle Brewery, Beach Road, Woodstock, Cape Town

T: +27 214476332

W: www.researchictafrica.net

This is policy brief was based on independent research and funded by Microsoft. The views and recommendations in this paper do not necessarily present the views of Microsoft on AI.