GLOBAL INFORMATION SOCIETY WATCH 2019

Artificial intelligence:
Human rights, social justice and development

Association for Progressive Communications (APC),
Article 19, and Swedish International Development Cooperation Agency (Sida)

Global Information Society Watch

2019

Global Information Society Watch 2019
Artificial intelligence: Human rights, social justice and development

Operational team
Valeria Betancourt (APC)
Alan Finlay (APC)
Mallory Knodel (ARTICLE 19)
Vidushi Marda (ARTICLE 19)
Maja Romano (APC)

Project coordination team
Valeria Betancourt (APC)
Cathy Chen (APC)
Flavia Fascendini (APC)
Alan Finlay (APC)
Mallory Knodel (ARTICLE 19)
Vidushi Marda (ARTICLE 19)
Leila Nachawati (APC)
Lori Nordstrom (APC)
Maja Romano (APC)

GISWatch 2019 advisory committee
Namita Aavriti (APC)
Rasha Abdul Rahim (Amnesty International)
Alex Comninos (Research ICT Africa)
Malavika Jayaram (Digital Asia Hub)
J. Carlos Lara (Derechos Digitales - América Latina)
Joy Liddicoat (Centre for Law and Emerging Technologies, University of Otago)
Andrew Lowenthal (EngageMedia)
Micaela Mantegna (Geekylegal/Machine Intelligence Lab, Center for Technology and Society, San Andres University)
Valeria Milanes (Asociación por los Derechos Civiles)

Project coordinator
Maja Romano (APC)

Editor
Alan Finlay (APC)

Assistant editor and proofreading
Lori Nordstrom (APC)

Publication production support
Cathy Chen (APC)

Graphic design
Monocromo

Cover illustration
Matías Bervejillo

We would like to extend a special note of thanks to a number of authors who have made ad honorem contributions to this edition of GISWatch.
We gratefully acknowledge the following:

Philip Dawson and Grace Abuhamad (Element AI)
Anita Gurumurthy and Nandini Chami (IT for Change)
Rasha Abdul Rahim (Amnesty International)

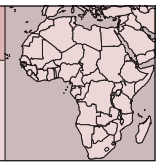
APC would like to thank the Swedish International Development Cooperation Agency (Sida) and ARTICLE 19
for their support for Global Information Society Watch 2019.

Published by APC
2019
Printed in USA

Global Information Society Watch 2019 web and e-book
ISBN 978-92-95113-13-8
APC Serial: APC-201910-CIPP-R-EN-DIGITAL-302

AFRICA

AI IN AFRICA: REGIONAL DATA PROTECTION AND PRIVACY POLICY HARMONISATION



Raymond Onuoha
Regional Academic Network on IT Policy (RANITP),
Research ICT Africa
https://researchictafrica.net/ranitp

Introduction

Basking in the ubiquitous adoption of mobile technology in Africa, experts in the technology domain prognose a similar upswing in the application of artificial intelligence (AI), especiall y in the communications space, and expect it to help leapfrog critical challenges on the continent.[1] With predictions of significant advancements relying on AI over the next 20 years,[2] there seem yet very sparse collective attempts by regional governments in Africa and the continent as a whole to deal with critical emerging issues. This is especially the case with regard to data protection and privacy, such as government surveillance or corporate influence over customers. Though the challenge of specific AI-related cyberpolicy formulation on the continent may appear unrealistic at this early stage, it is imperative to initiate critical discussions on the context-specific requirements with regard to adapting existing or formulating new regulatory policy as it pertains to AI.

State of play: Regional data protection and privacy policy frameworks in Africa

The adoption and effective implementation of existing data protection and privacy policy frameworks by countries across Africa – even with the limitations on the continent with respect to AI developments – is still a fundamental reference point for ensuring that critical safeguards are in place while we seek to maximise the benefits of AI. The closest continent-wide policy document in this regard – the African Union's (AU) 2014 Malabo Convention on Cyber Security and Personal Data Protection[3] – has been signed by just 11 out of the 55 member countries (these are Benin, Chad, Comoros, Congo, Ghana, Guinea-Bissau, Mozambique, Mauritania, Sierra Leone, Sao Tome and Principe and Zambia), while only three member countries (Guinea, Mauritius and Senegal) have ratified the policy document. While the convention provides "fundamental principles and guidelines to ensure an effective protection of personal data and [seeks to] create a safe digital environment for citizens, security and privacy of individuals' data online," it makes no reference to institutional strategies of mitigating the threats posed specifically by AI deployments on the continent.

At the regional level, the focus has largely been on the policy element of data privacy, with the Economic Community of West African States (ECOWAS) leading the way via the 2010 Supplementary Act on Personal Data Protection within ECOWAS.[4] Similar, albeit non-binding policy instruments have also been developed by the East African Community (EAC) – the 2012 Bill of Rights for the EAC[5] and the 2011 draft EAC Legal Framework for Cyber Laws.[6] In the same regard, the Southern African Development Community (SADC) established the Model Law on Data Protection in 2012,[7] but it is non-binding on member states, making implementation and enforcement difficult.[8] However, disharmony at the regional level with respect to policy formulation generally undermines levels of compliance. This situation demands more continent-level coherence for easier adoption and implementation. If it persists

1 Bostrom, N., Dafoe, A., & Flynn, C. (2018). *Public Policy and Superintelligent AI: A Vector Field Approach*. Oxford, UK: Governance of AI Program, Future of Humanity Institute, University of Oxford. https://pdfs.semanticscholar.org/9601/74bf6c840bc036ca7c621e9cda20634a51ff.pdf; Dafoe, A. (2018). *AI Governance: A Research Agenda*. Oxford, UK: Governance of AI Program, Future of Humanity Institute, University of Oxford. https://www.fhi.ox.ac.uk/wp-content/uploads/GovAIAgenda.pdf; Gadzala, A. (2018). *Coming to Life: Artificial Intelligence in Africa*. Washington: Atlantic Council. https://www.atlanticcouncil.org/images/publications/Coming-to-Life-Artificial-Intelligence-in-Africa.pdf

2 Turianskyi, Y. (2018). *Balancing Cyber Security and Internet Freedom in Africa*. South African Institute of International Affairs. https://www.africaportal.org/publications/balancing-cyber-security-and-internet-freedom-africa

3 https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

4 www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf

5 www.eala.org/documents/view/the-eac-human-and-peoples-rights-bill2011

6 repository.eac.int:8080/bitstream/handle/11671/1815/EAC%20Framework%20for%20Cyberlaws.pdf?seq

7 www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/SA4docs/data%20protection.pdf

8 Turianskyi, Y. (2018). Op. cit.

as it is, the disharmony inadvertently increases the gap between the frontiers of global technology and mechanisms of local and regional governance that has geopolitical ramifications for the continent.[9]

Institutional challenges for regional/ continental data protection policy harmonisation in Africa

The recent and rapid diffusion of the internet across Africa, with the attendant emergence of AI deployments on the continent, is growing ahead of institutional, social and cultural changes. In this purview and in specific relation to data protection and privacy policy institutionalisation, currently only 17 out the 55 member countries of the AU have enacted comprehensive data protection and privacy legislation (these are Angola, Benin, Burkina Faso, Cape Verde, Gabon, Ghana, Ivory Coast, Lesotho, Madagascar, Mali, Mauritius, Morocco, Senegal, Seychelles, South Africa, Tunisia and Western Sahara).[10] This slow pace of data governance policy evolution among AU member countries has been identified as a major hindrance to a harmonised policy framework for data protection and privacy. Of note in this regard, the number of countries in Africa that have enacted comprehensive data protection and privacy legislation is even more than the number that have adopted the continental-level Malabo Convention with respect to data protection and privacy. Most of the national data protection laws also existed before the Malabo Convention and seem to have more specific details with regard to data protection than the AU convention and addressing the issues that have subsequently emerged. This is one concern with the Malabo Convention that has been raised by AU member countries.

A challenge with respect to the continental-level data policy process is that it is a very slow and painstaking process. As a result, although less than half the countries on the continent have implemented policies on data, many have been forced to move ahead without necessarily looking to the region for guidance. In addition, with the largely top-down approach of data policy engagement by the AU and the Regional Economic Communities (RECs), with people just making laws on behalf of countries, regional instruments are bound to run into significant adoption challenges. In this light, research indicates that a top-down regional policy engagement process might only be designed to "serve narrow regime interests at the expense of broader national and collective interests."[11]

Another challenge impacting the adoption of the AU Malabo Convention is the lack of sector or industry-specific considerations with regard to data protection and privacy guidelines akin to the European model laws. This creates unhelpful levels of uncertainty and unpredictability, especially for multinational organisations seeking compliance within national boundaries.[12]

A critical hindrance to data protection and privacy policy cooperation on the continent is the significant variation in cultural and legal diversity, access to technology, and governance capacity for data-related policy making.[13] Compounding this problem is the existing legacy allegiance of the regional blocs within the AU to their former colonial countries in such a manner that sharply divides the policy interests of the Anglophone and Francophone countries, thereby weakening the cohesiveness of the continental body in general with respect to data policy making.

This situation makes Africa's relationship with data governance unclear – a lack of clarity that is compounded by capacity constraints. The policy-making institution in Africa is largely led by a traditionally analogue generation that predates the internet age, making the understanding of data-led digital policy engagements challenging. There is therefore a lack of capacity and understanding of who should take responsibility in the region with regard to data-driven technology and its imperatives with respect to digital rights. This general lack of understanding leads to a lack of policy direction with respect to emerging issues such as AI.

The existing lack of capacity and technical expertise at the policy-making echelon for data governance in Africa poses a significant implementation and process management cost to a harmonised regional policy framework. Further training and

9 Evanoff, K., & Roberts, M. (2017, 7 September). A Sputnik moment for artificial intelligence geopolitics. *Council on Foreign Relations*. https://www.cfr.org/blog/sputnik-moment-artificial-intelligence-geopolitics

10 Mabika, V. (2018, 8 May). The Internet Society and African Union Commission Launch Personal Data Protections Guidelines for Africa. *Internet Society*. https://www.internetsociety.org/blog/2018/05/the-internet-society-and-african-union-commission-launch-personal-data-protections-guidelines-for-africa

11 Söderbaum, F., Skansholm, H., & Brolin, T. (2016). *From top-down to flexible cooperation: Rethinking regional support to Africa*. The Nordic Africa Institute. cris.unu.edu/sites/cris.unu.edu/files/From%20Top%20Down%20to%20Flexible%20Cooperation%20-%20May%202016.pdf

12 Ridwan, O. (2019, 20 March). 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*. https://aanoip.org/the-africa-continental-free-trade-agreement-and-cross-border-data-transfer-maximising-the-trade-deal-in-the-age-of-digital-economy

13 Mabika, V. (2018, 8 May). Op. cit.

assistance for policy makers may be required; more so as a large number of AU member countries are yet to establish independent data privacy regulatory authorities. Bridging this capacity gap among policy makers within the AU region is imperative, as an unclear understanding of emerging technological developments with respect to data policy might produce the unintended consequences of limiting the region's competitiveness in the AI economy. This is of importance when it comes to issues such as data availability for multinational organisations operating on the continent that collect, process and share data for AI-based applications and services, especially those that are mobile phone based. For example, a forced data localisation regime on the pretext of maintaining national security and sovereignty might restrict cross-border data transfers for such multinational data companies who may choose to move their foreign direct investment to more favourable destinations.

In the final analysis, with regard to priorities, many African countries are still dealing with basic issues of sustenance like food and housing, etc., so technology and technology policy are not at the front burner of critical issues of concern. According to one regional policy expert interviewed for this report, "A government that is still battling [to set up a] school feeding programme in 2019 is not going to be the one to prioritise data and data protection policies with respect to AI." A harmonised regional data protection policy regime for the continent might impose enforcement liabilities on member countries that lack the required resources for its implementation.[14] These costs would be in the form of funds necessary for setting up data protection authorities at the governmental levels as well as designated data privacy representatives for private sector players. Furthermore, in as much as a continent-wide data protection and privacy policy framework for Africa will catalyse regional collaboration and cooperation in dealing with the emerging issues and risks posed by AI deployments on the continent, it may however impose costs and raise conflicts with other national data protection and privacy regimes if it is not well harmonised globally. So the Malabo Convention is indeed a good place to start, but then again the AU will need to do a lot more work in promoting its benefits not just regionally, but within an emerging global policy context.

14 Curtiss, T. (2016). 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, 12*(1). digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/1654/12WJLTA095.pdf?sequence=4&isAllowed=y

Conclusion

The growing shift towards a more centralised data protection and privacy policy framework in Africa considering the significant cross-border imperatives of AI deployments, as well as cross-sectoral technological developments, comes with critical challenges. Regulators on the continent need to become more innovative and seek to understand emerging AI technologies in order to effectively regulate them. They need to consider AI-related principles that would apply contextually irrespective of the technologies or systems that are deployed. Not all policy needs with respect to AI are complex – some are pretty straightforward to implement. A good example here is driving the adoption of AI-related data policy in the continent by matching AI technology with the socioeconomic needs that are addressable in peculiar contexts within the region. It is nevertheless necessary to have stakeholders with a shared understanding of the policy needs and on the same page with regard to a clear direction of where the continent wants to go, and how its respective countries can benefit from this path. People need to become more aware with respect to the critical issues of transparency and openness. They need to know that there are built-in safeguards to protect their personal data that are collected from misuse, especially in line with the principle of making sure that further processing of their personal data is compatible with the reasons or basis for which they were collected in the first place. These remain fundamental in building trust within the technology ecosystem. Furthermore, and in consideration of the longer term, a coherent regional data policy framework for the region should be technologically neutral with consistencies across multi-industry sectors and services. However, risk assessment models should be built into the regional frameworks in such a way as to reflect accepted privacy principles.

In adapting current regional data protection frameworks in Africa to deal effectively with the emerging challenges of AI, there are many lessons that Africa needs to learn from other regions that have moved forward earlier with policies and practices relevant to data protection and related cyberpolicy.

While the European Union's General Data Protection Regulation (GDPR) is a model for regional data protection policy collaboration, it can be improved on and not just taken as a silver bullet solution for the continent. Nevertheless, many of its requirements are worth adopting. For example, considering the cross-border imperatives of AI systems, regional

data policy instruments should be framed in such a way that data-handling firms operating in Africa must be made to sign up to the data protection and privacy laws within their operational jurisdictions, whether or not they are registered as a business entity in those jurisdictions. This is of significant importance for Africa considering the fact that critical data-related projects across the continent are handled and processed outside her borders. Some key examples in this regard include the Kenya Digital ID project,[15] which is hosted and processed by a foreign company, and the data collected by Ghana's Electoral Commission, which is not hosted in-country. Moreover, none of the big data firms – Facebook, Google, Amazon and Microsoft – are registered as business entities in any African country.

Action steps

The following action steps are suggested for civil society:

- *Capacity building for effective policy making*: Africa has been saddled with the burden of leaders who are behind technology advancements. Keeping pace with evolving technologies will require policy evolution and adaptations. Civil society can help in bridging these capacity deficits in such a manner that cross-country peculiarities and spillovers are taken into consideration. They can engage in the build-out of AI knowledge centres[16] across the region that will help bridge these critical gaps by encouraging a thorough understanding of the issues involved, and serve as a resource to help understand the policy directions of the various RECs with respect to AI.
- *Pushing for AI-related principles and values in data protection policy:* Data protection laws and frameworks are built on general principles, like most technology laws, which are developed to regulate appropriate behaviour regardless of technology evolution with time. However, AI involves a number of specific issues that need to be addressed. Civil society can advocate for appropriate contextual principles and values around which the regional entities can coordinate on data protection policy relevant to AI. Critical among these principles for Africa is the right to privacy of an individual, which is fundamental for our existence as human beings. Furthermore, people need to become more aware with respect to transparency and openness. Another principal area of concern with regard to AI policy is the issue of bias, as AI is currently being developed in primarily two regions of the world: the West and China/Russia. In each of these regions, there is a paucity of data being fed into AI machines that correlates with the African experience. Furthermore, AI data policy for the continent must not be a one-sided issue; it has to be gender-centric and also take into consideration marginalised groups as well as the diversity of different languages and cultures within the region in order to achieve a broad-based result that engenders equitable technology access.
- *Socioeconomic needs assessment*: Civil society can advocate for the adoption of relevant AI-related data policy by helping to match it to the socioeconomic needs in particular contexts in the region. A needs analysis of countries must be done with respect to AI technology so policy can be linked to economic solutions. AI is useless to African countries if it is not applied in a way that solves their needs.
- *Multistakeholder policy advocacy:* Civil society can contribute to a multistakeholder process that also includes governments, citizens, universities and the private sector to help collaboratively adapt current regulatory frameworks in such a manner that they promote digital innovation while protecting the privacy and security of citizens.

15 Dahir, A. L. (2019, 21 February). Kenya's plan to store its citizens' DNA is facing massive resistance. *Quartz*. https://qz.com/africa/1555938/kenya-biometric-data-id-not-with-mastercard-but-faces-opposition

16 Such as the Global Cyber Security Capacity Centre pioneered by the University of Oxford. https://www.oxfordmartin.ox.ac.uk/cyber-security

GLOBAL INFORMATION SOCIETY WATCH 2019

Artificial intelligence:
Human rights, social justice and development

Artificial intelligence (AI) is now receiving unprecedented global attention as it finds widespread practical application in multiple spheres of activity. But what are the human rights, social justice and development implications of AI when used in areas such as health, education and social services, or in building "smart cities"? How does algorithmic decision making impact on marginalised people and the poor?

This edition of Global Information Society Watch (GISWatch) provides a perspective from the global South on the application of AI to our everyday lives. It includes 40 country reports from countries as diverse as Benin, Argentina, India, Russia and Ukraine, as well as three regional reports. These are framed by eight thematic reports dealing with topics such as data governance, food sovereignty, AI in the workplace, and so-called "killer robots".

While pointing to the positive use of AI to enable rights in ways that were not easily possible before, this edition of GISWatch highlights the real threats that we need to pay attention to if we are going to build an AI-embedded future that enables human dignity.

GLOBAL INFORMATION SOCIETY WATCH
2019 Report
www.GISWatch.org

APC
ARTICLE 19
Sida