

THE CONVERSATION

Academic rigour, journalistic flair



Getty Images/akinbostanci

AI regulation in Africa: why copying the European model won't work

Published: June 10, 2026 2.37pm BST

<https://theconversation.com/ai-regulation-in-africa-why-copying-the-european-model-wont-work-283524>

Mauritius set out its national AI strategy in 2018, the first by an African country. Since then over a dozen African states have adopted national AI policies of some sort or another.

As a national policy plan, an AI strategy typically sets out the priorities and aspirations in achieving certain policy objectives.

At the continental level, the African Union has adopted an [AI strategy](#).

Kenya and Ethiopia have tabled draft AI laws that set out how the countries want AI governed. [Morocco](#), [Egypt](#) and [Nigeria](#) are already mulling the idea of AI legislation. The trend shows that policymakers are slowly turning their attention from unchecked enthusiasm about AI to reckoning with governing AI risks.

As technology law and policy scholars, our research explores the dynamics of and approaches to the governance of emerging technologies like AI. Our recent [work](#) explores the origins, nature and scope of AI governance initiatives in Africa. We found a number of common threads in recent policy and legislative exercises. One such trend is for African states to adopt the European Union's approach to AI regulation. But this needs to be called into question.

No doubt, Africa needs AI legislation. It will be vital to regulate the development and use of AI systems that pose risks to individual rights, social cohesion or even national security. Legislation can also create new regulatory bodies that oversee AI rules or other relevant laws such as data protection.

Kenya's [AI Bill](#), for instance, institutes the AI Commissioner as well as the AI Advisory Committee as regulators of AI systems in the country.

But the effort to turn AI policies into legislation requires reckoning for two reasons.

More laws, less implementation

One concern is whether the continent really needs a new layer of digital laws while preceding pieces of tech legislation remain largely unenforced. AI policies were meant to coordinate AI development at the national level. While some countries committed to responsible AI development, others have yet to set up or fund institutions that were to give the strategies meaning.

This points to an endemic problem in Africa: lack of implementation. Data protection is a case in point. Many African countries have enacted data protection legislation but are yet to install oversight bodies, or those established lack the resources to enforce laws.

Legislating for AI in this environment risks producing laws that will largely be aspirational in the same way as the strategies before them: they are there but aren't implemented.

Europeanisation of African law

The second concern relates to the heavy reliance on European standards in fashioning emergent AI laws. Both Kenya's and Ethiopia's AI bills adopt the European Union's risk-based approach. This involves regulating AI systems based on the nature of risk they pose. Those posing "unacceptable risks" are banned altogether and those with lower risks have to meet requirements.

Transplanting European standards is not new in African states' attempt to regulate new and emerging technologies. The first generation of data protection and cybercrime laws in Africa drew directly from formative legal instruments in Europe. But rarely have such legal transplanting exercises been informed by or taken into account local contexts, interests and concerns. Perhaps this is why data protection standards aren't implemented effectively.

The concern is not that the EU's approach is inherently problematic. It's why African states fail to envision an approach informed by local realities. AI regulation in Africa should not emerge from a compulsion to signal regulatory modernity. Laws calibrated for mature digital markets, well-resourced regulators, and rights aware consumer populations do not translate cleanly into contexts defined by thin institutional capacity, informal data flows, and populations with limited ability to exercise the rights those laws nominally protect.

Grounding regulation in reality

African states need AI laws based on a concrete and honest reckoning with what AI is actually doing or could do to the continent. Fashioning AI regulation should be preceded by critical reflection on the following key questions:

- How is it being deployed by technology companies? How is information and misinformation spread on the continent?

- How is it being used in public services? Who benefits when governments deploy AI in social protection, policing, or public administration?
- Who controls the data? Large technology companies, many of them headquartered in the United States, China, or Europe, are able to collect and process vast amounts of data generated by African users. This is often done under terms of service that most users neither read nor meaningfully consent to, and with little accountability to African regulators.
- Who bears the harms? Who bears the risk when those systems get it wrong?
- Whose interests are unprotected? AI-powered content moderation systems, for example, perform poorly in African languages and local contexts.

Imperatives of moratorium

As the AI hype continues, African states are already deploying AI in different sectors, including healthcare. [Ethiopia](#) and [Rwanda](#), for example, used AI in TB and cervical cancer screening. But it's happening in a regulatory vacuum. In the absence of a robust regulatory regime, AI is likely to cause considerable harm to individuals and societies.

While AI legislation might be a promising step forward in filling the regulatory void, this effort appears to be restricted only to a few countries whose approach is yet to move past European parameters. Policymakers should rather prioritise pursuing a more considered and contextualised approach to address AI risks meaningfully.

Until then, a moratorium on the use of high-risk AI systems in sensitive domains such as healthcare should be seriously considered.

Kinfe Yilma

Senior Lecturer, University of Leeds

Grace Mutung'u

Research Fellow, Centre for Intellectual Property and Information Technology Law (CIPIT), Strathmore University

DOI

<https://doi.org/10.64628/AAJ.cafqvkwn>