

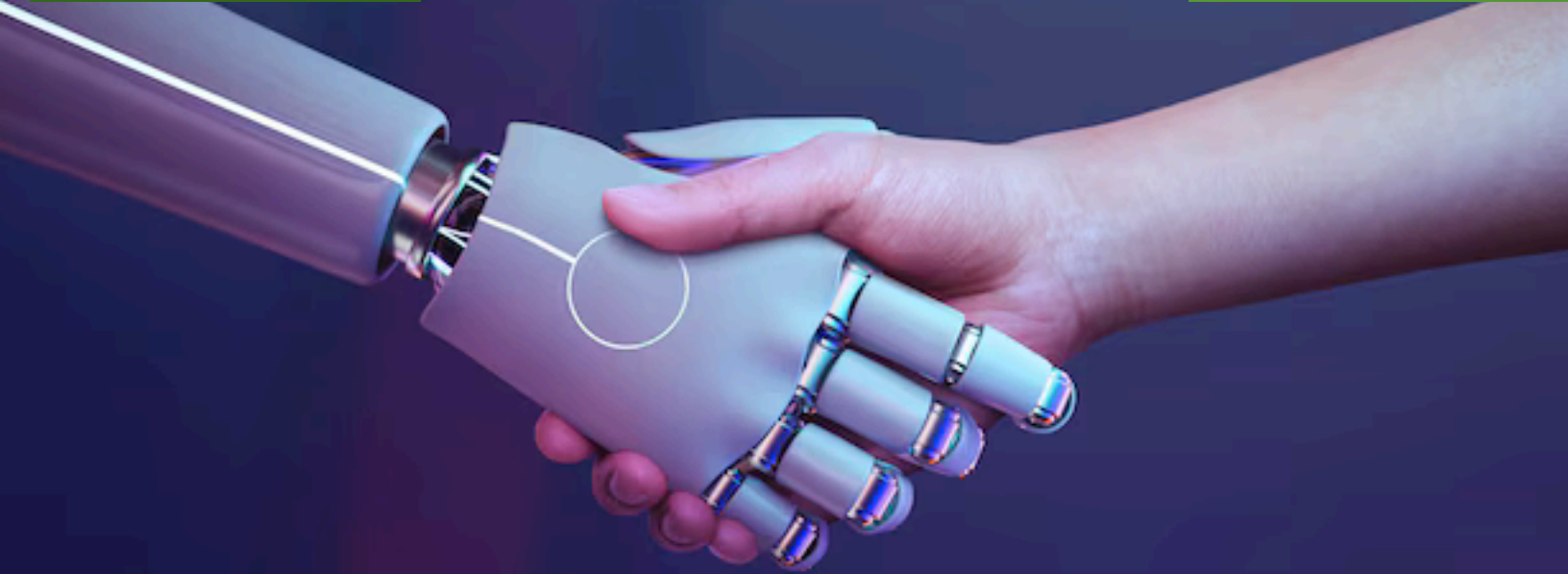


INTERNATIONAL LAW ASSOCIATION  
COMMITTEE ON ARTIFICIAL INTELLIGENCE, NEW  
TECHNOLOGIES AND INTERNATIONAL LAW

**3-PAGE BRIEF**

# ILA COMMITTEE ON ARTIFICIAL INTELLIGENCE, NEW TECHNOLOGIES AND INTERNATIONAL LAW

<https://ila-aitechlaw.org>



## RESPONDING TO HUMAN RIGHTS RISKS IN THE CONTEXT OF LINKED TO PROCUREMENT OF ARTIFICIAL SYSTEMS BY AFRICAN STATES

### INFORMATION BRIEF



### AUTHORS

Omolara OLANIBUKUN, Freedolyn ANI, Abel NDUKA, Ogona ANNETTE, Israel ADENIYI, ETIMBUK Philip, Adachukwu MADUEME, Adekunle OLAJIDE, Ukechi Ihuoma JACKSON-WALI and Shitta BUSOLAMI, Tomi FAKOS, Abdulhakeem JAYEOLA, Adama THERESA, Sofiyah OSHODI, Favour DULYAMBA, Oluwadamilola EKUNDAYO, Karimat ABDULAZEEZ, Praise ADEGOKE, Emediong AKPAN, Abdulbasit OLAWALE O., Apostle Nkem AMAECHI-NDUKWE, Yusuf EEMAN, QUAM Abdulganiyu, Gbopemioluwa OLUKOGA, Ayotunde ABIODUN, Deborah OTIGHI, Waliyat SALIU.

THIS BRIEF WAS PREPARED FOR THE UN WORKING GROUP ON BUSINESS AND HUMAN RIGHTS TO INFORM THE WORK OF THE GROUP ON THE USE OF ARTIFICIAL INTELLIGENCE AND THE UN GUIDING PRINCIPLES ON BUSINESS AND HUMAN RIGHTS.

THE BRIEF WAS PREPARED UNDER THE DIRECTION OF DR ADEROMOLA ADEOLA (ILA AI, NEW TECHNOLOGY AND INTERNATIONAL LAW COMMITTEE CHAIR) AND SUPERVISED BY MR TOM UTUM (YOUTH-SUB COMMITTEE LEAD). THE COMMITTEE EXTENDS AN APPRECIATION TO PROF DAMILOLA OLAWUYI, THE INTERNATIONAL LAW ASSOCIATION (NIGERIA) PRESIDENT FOR HIS SUPPORT.

THIS BRIEF WAS PREPARED BY THE INTERNATIONAL LAW ASSOCIATION (NIGERIA BRANCH) COMMITTEE ON ARTIFICIAL INTELLIGENCE, NEW TECHNOLOGIES AND INTERNATIONAL LAW. THE AUTHORS OF THIS REPORT ARE PART OF THE 2025 YOUNG PROFESSIONAL PROGRAM COHORT. THEIR SPECIFIC NAMES ARE INCLUDED IN THIS STUDY. FOR MORE INFORMATION, PLEASE VISIT: [HTTPS://ILA-AITECHLAW.ORG](https://ila-aitechlaw.org)

## Theme One: Privacy as a concern

There are several human rights risks linked to procurement and deployment of AI systems across the continent. A major risk that resonates across many African countries is privacy. The extensive collection and utilization of personal data by AI-powered applications have raised significant privacy concerns, as data protection regulations in many African nations remain underdeveloped.

For example, AI-powered credit-scoring tools used by microfinance institutions have raised concerns across some countries. There have been concerns about AI-driven recruitment and credit-scoring platforms exhibiting gender and ethnic biases, denying qualified individuals access to employment and financial opportunities. These tools collect data from online sources, such as social media sites, without the explicit consent of users. The lack of transparency and consent erode individuals' rights to privacy.

While at least 37 countries have laws on privacy, what really needs to be enhanced is implementation. Another evident risk is algorithmic bias and in response to this, there needs to be an emphasis on transparency, enhanced access to information regimes, and an emphasis on the explainability of AI systems.

## Theme Two: Laws and Policies

Africa has a Continental Artificial Intelligence Strategy, which was adopted in 2024. Across Africa, countries are beginning to develop laws, policies and institutions on AI. Kenya has a National Digital Master Plan from 2022-2032. Egypt developed a National AI strategy in 2021. In August 2024, Nigeria adopted a National Artificial Intelligence Strategy. It also has a National Center for AI and Robotics on AI technologies.

What resonates across a plethora of countries is the existence of law and policy frameworks that are crucial to AI, specifically data protection laws. Many countries across Africa have developed robust data protection. Nigeria adopted a Data Protection Act in 2023, South Africa has a Protection of Personal Information Act (POPIA), Ghana has Data Protection Act of 2021 and Chad also developed a Law No 007 of 2015. Ethiopia developed a Personal Data Protection Act in 2024. At least 37 African countries have data protection laws.[1]

While these laws present opportunities for AI governance, there is a need for specific AI law and policies. And the current landscape on development presents good opportunities for infusing perspectives on human rights risks and protection.

[1] The state of data protection legislation in Africa  
<<https://www.techpolicy.press/the-state-of-data-protection-legislation-in-africa/>>

## Theme Three: Emerging good practice

Across Africa, tech companies are adopting ethical AI frameworks, through which they are infusing rights-based consideration including privacy.

A good example of a business doing this on the continent is MTN. MTN has a Digital Human Rights Policy that draws on the UN Guiding Principles on Business and Human Rights.[2] It is explicit on the fact that its approach is guided by the framework and respects the AU Convention on Cyber Security and Personal Data Protection. Moreover, it offers a clear grievance mechanism for customers to report issues via [humanrights@mtn.com](mailto:humanrights@mtn.com) with a commitment to investigate and address violations promptly.

To ensure these practices are prevalent, it is important to create platforms for regular stakeholder engagement. The reason we emphasize this is because it affords a basis for collaboration among stakeholders in addressing human rights impacts and enhancing the co-creation of solutions. Creating such platforms can also be used to advance AI explainability and foster transparency.

[2] MTN Group, 'MTN Position Statement' <<https://www.mtn.com/wp-content/uploads/2024/04/MTN-Position-on-DHR.pdf>> accessed 11 January 2025

## Theme Four: Decisions-relevant to AI governance

As the landscape on AI is emerging, decisions on the subject-area will significantly emerge in the near future.

However, there are important pronouncements on privacy rights. For instance, the *Nubian Rights Forum & 2 Ors v. Attorney General of Kenya & 6 others* is instructive.[3] The authors of the case challenged the National Integrated Identity Management System (Huduma Namba) which they argued was an excessive infringement on the right to privacy. Among others, it required the collection of DNA and GPS information.

Though the Kenyan government passed a Data Protection Act, the court ordered the state to develop a robust framework that guaranteed the right to privacy.

[3] Petition 56, 58 and 59 of 2019 (Consolidated); [2020] eKLR <[https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2021/10/Petition\\_56\\_58\\_59\\_of\\_2019\\_Consolidated.pdf](https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2021/10/Petition_56_58_59_of_2019_Consolidated.pdf)>