Digital Colonialism and Data Sovereignty

AiCE Africanism & Pan-African Studies — Who owns Africa's data?

Who Owns Africa's Data?

As African economies and societies become increasingly digital — as more transactions, communications, health records, agricultural data, and government services move online — a new form of colonial extraction is taking shape. This is data colonialism: the extraction of African data by foreign corporations and governments, and its use to generate value — economic, political, and strategic — that flows primarily outside Africa rather than serving African development.

The mechanisms of data colonialism are visible in the everyday digital lives of Africans. The social media platforms billions of Africans use to communicate, organise, and conduct business — Facebook, WhatsApp, TikTok, Twitter/X — are owned by American and Chinese corporations. Every post, every message, every click generates data these companies collect, analyse, and monetise. The advertising revenues generated by African users flow to Silicon Valley and Beijing. The data itself — increasingly the most valuable raw material in the global economy — is stored on servers outside Africa, governed by foreign laws, and used to train artificial intelligence systems that serve foreign interests.

Nick Couldry and Ulises Mejias, in their 2019 book Data Colonialism: Thickening Convergences of Digital Data and Racial Capitalism, argue this data extraction represents a new form of colonial appropriation — analogous in structure to the colonial extraction of land and labour, but operating through digital rather than physical means. Just as colonial economies were structured to extract African resources for foreign benefit, the digital economy is structured to extract African data for foreign benefit. The value of what is taken vastly exceeds the value of what is received in return.

Digital Colonialism: Key Dimensions
Platform dominance: the major digital platforms Africans use are foreign-owned; advertising revenues from African users flow outside Africa.

Digital Colonialism: Key Dimensions
Data extraction: African user data is collected and stored outside Africa, used to train AI systems and target advertising without meaningful consent or compensation.
Undersea cable control: the cables carrying Africa's internet traffic are largely owned by foreign corporations, including Google and Facebook.
Cloud dependency: African governments and businesses increasingly store data on foreign cloud platforms, creating dependency and jurisdictional vulnerability.
AI training data: African faces, voices, languages, and cultural expressions are used to train foreign-owned AI systems without compensation to African communities.
Algorithmic governance: social media algorithms designed for Western markets moderate African content by Western norms, often suppressing African political speech.
Financial data: African mobile money and banking data is increasingly captured and analysed by foreign fintech companies.

Building African Data Sovereignty

The response to data colonialism must be African data sovereignty — the principle that African data should be governed by African institutions, stored in Africa, and used primarily to serve African development. This is not protectionism or technological isolationism. It is the digital equivalent of what Nkrumah argued for mineral resources: African resources should be controlled and developed by Africans, for Africans.

Several African countries have taken significant steps toward data sovereignty. Rwanda's Data Protection Act (2021) establishes strong protections for personal data and requires appropriate security measures. Nigeria's Data Protection Regulation (2019), now being strengthened into a full Data Protection Act, establishes rights for Nigerian data subjects and obligations for data controllers. South Africa's Protection of Personal Information Act (POPIA, 2021) is among the most comprehensive data protection frameworks on the continent.

The African Union's Data Policy Framework (2022) provides a continental-level framework for data governance, aiming to harmonise national approaches and ensure African data serves African development, explicitly addressing the risk of data

colonialism and calling for African data to build African AI systems, African research capacity, and African economic opportunity.

Building genuinely sovereign African digital infrastructure requires more than legislation. It requires African-owned data centres and cloud infrastructure, African-owned social platforms that can compete with foreign alternatives, African-developed AI systems trained on African data and serving African needs, and African regulatory capacity to enforce data protection standards against powerful foreign corporations. All of these are long-term projects. But they have begun.

Key Takeaways

Data colonialism extracts African data — through foreign-owned platforms, cables, clouds, and AI systems — with the value flowing overwhelmingly outside Africa, structurally analogous to colonial resource extraction. African data sovereignty legislation in Rwanda, Nigeria, and South Africa, backed by the AU's continental Data Policy Framework, represents the beginning of a response, though building genuinely sovereign digital infrastructure remains a long-term project. The next lesson examines a technology where the stakes are especially high: artificial intelligence.