Centre for International
Governance Innovation

Policy Brief No. 238 — May 2026

AI and Refugee Protection in the African Union: Smart Borders or Fortress Africa?

Jake Okechukwu Effoduh

Key Points

- Artificial intelligence (AI)-driven border technologies, including biometrics, drones, predictive analytics and automated risk scoring, are already used in several African Union (AU) member states. Ghana, Kenya and South Africa illustrate a broader continental shift toward technology-enabled border governance.
- The AU *Continental Artificial Intelligence Strategy* sets a framework for Africa-centric AI governance but implementation is uneven, with few national strategies and variable progress on data protection commitments.
- EU border externalization policies influence African border governance through funding, operational cooperation and technology transfers that integrate African systems into transnational surveillance and data-sharing architectures.
- Weak data sovereignty, biometric bias and limited oversight pose risks to privacy and refugee protection. Algorithmic impact assessments (AIAs), independent oversight and stronger data governance are needed to align AI border systems with security goals and fundamental rights.

Introduction

In July 2024, the AU Executive Council endorsed the *Continental Artificial Intelligence Strategy* at its forty-fifth ordinary session in Accra, Ghana, marking Africa's most comprehensive effort to harness AI for socio-economic transformation while asserting technological sovereignty (African Union 2024). The strategy, with implementation phases extending from 2025 to 2030, envisions AI-driven transformations across health care, agriculture, education, public services and, notably, governance and security sectors, including border management (ibid.). It arrived at a critical juncture, given that across the continent, AU member states are already deploying AI-driven border technologies (including biometric systems, drone surveillance, predictive analytics and interoperable data platforms), in response to real security concerns linked to trafficking, smuggling and irregular migration.

Ghana, Kenya and South Africa illustrate this trend. In September 2025, Kenya unveiled a comprehensive border security modernization strategy targeting its frontiers with Somalia and Ethiopia, deploying drones equipped with AI-powered thermal detection, biometric identity verification systems and interoperable platforms that enable real-time

About the Author

Jake Okechukwu Effoduh is a CIGI senior fellow and an assistant professor at the Lincoln Alexander School of Law, Toronto Metropolitan University. His research focuses on the intersections of artificial intelligence (AI), human rights and international law. He has contributed his expertise to a broad range of AI policy development issues across Africa and countries such as Brazil, Canada, China and the United States.

He has carried out legal advocacy within sub-regional and regional systems such as the Economic Community of West African States Community Court of Justice, the East African Court of Justice, the African Commission on Human and Peoples' Rights and the United Nations Human Rights Council. Jake received the Social Sciences and Humanities Research Council Explore Grant for his work, Codes for Algorithmic Justice, which evaluated regulatory solutions for algorithmic bias against Black Canadians in the diaspora, and he is an inaugural recipient of the Black-Focused Pedagogy Grant for his work on critical race theory and Afrofuturism in AI and the law.

He is also the convener of Black Futures by Design, a conference advancing racial justice in AI governance and regulation; and a United Nations Educational, Scientific and Cultural Organization expert on AI and the rule of law, providing training to judges, law teachers and legal officers on the use of AI in legal and judicial contexts. A Rogers Cybersecure Catalyst fellow, Jake has also previously held fellowships at Harvard Law School, Harvard Kennedy School, Carnegie Mellon University, the University of Ottawa and the University of Cape Town. He serves as editor-in-chief of the *Transnational Technology Law Review* and as an editor of the *Transnational Human Rights Review*.

intelligence sharing among security agencies. South Africa's Border Management Authority reported a 63 percent increase in interdiction success during the 2025 Easter period, following the deployment of AI-powered drones equipped with night-vision and thermal-detection capabilities (SAnews.gov.za 2025). Similar technologies are increasingly being deployed across extended land borders and remote crossings, where drones, sensors and biometric identification systems allow authorities to monitor large areas that were previously difficult to patrol. These developments reflect a broader continental shift toward technologically mediated border governance.

Yet this technological transformation unfolds within a broader political economy that extends beyond the African continent. EU border externalization policies — through which the European Union funds and supports migration control measures in non-EU countries to prevent irregular migration before it reaches European territory — have expanded operational cooperation with African states. Frontex, the European Border and Coast Guard Agency responsible for coordinating EU external border management, now operates in or cooperates with authorities in Mali, Mauritania, Niger, Senegal, and other countries. At the same time, the Migration Information Data Analysis System (MIDAS) — a border management platform developed by the International Organization for Migration (IOM) and deployed in Nigeria with European funding — supports the collection and processing of traveller data. Similar biometric registration programs in Mauritania capture data from migrants originating largely from Gambia, Guinea, Mali, Nigeria and Senegal.

Together, these systems form an increasingly integrated surveillance architecture that stretches from African transit states to European borders. Information collected through border management and biometric systems can circulate through migration management and law-enforcement cooperation channels involving actors such as IOM, Europol and Frontex. The effect is to position some African states as an upstream layer of migration control for Europe. In this sense, current developments point toward what may be described as a "Fortress Africa" trajectory, emerging through the interaction of domestic technological deployments, externally funded surveillance infrastructure and still-limited safeguards for rights, accountability and data governance.

This policy brief examines three interrelated questions. First, how do AI-driven border technologies serve AU member states' legitimate security interests, and what risks do they pose to privacy, data protection and fundamental rights? Second, how can AU member states reconcile their obligation to secure borders with their commitment to refugee protection under the 1969 Organisation of African Unity (OAU) Refugee Convention?[1] Third, how might the growing deployment of border technologies, combined with external cooperation and technology transfers, reshape patterns of migration governance across the continent, including the possibility of increasingly restrictive and technologically mediated border regimes sometimes described as a Fortress Africa dynamic? This brief argues that rights-based AI border governance requires at least four immediate safeguards: robust AIAs, independent oversight with meaningful civil society participation, stronger data sovereignty protections, and closer alignment with the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) and Africa's refugee protection commitments.[2]

Security Imperatives and Technological Capabilities

The security rationale for AI-driven border technologies in Africa seems substantial. Many AU member states confront porous borders with limited or no customs management systems across their full territorial extent. Illegal trafficking in drugs, weapons and human beings flourishes across territories where state border management is weak or absent, including in remote areas and regions under the control of non-state armed groups rather than central authorities, posing genuine threats to both national security and economic development. The AU High-Level Panel on Emerging Technologies has identified key weaknesses, including inadequate border control management systems and data sharing between member states; insufficient capacity to detect the smuggling of small arms and narcotics; growing human trafficking networks; weak governance of cross-border trade; and uncoordinated decision making among security officials (Dugbazah et al. 2021).

AI-driven technologies, alongside other advanced border surveillance systems, may offer genuine capabilities to address some of these challenges. Automated licence plate readers and biometric identification systems can strengthen identity verification at points of entry. Integrated fixed towers and perimeter intrusion detection systems employing sensor arrays and camera networks can monitor vast stretches of otherwise poorly governed or remotely administered borderlands. Unmanned aerial vehicles equipped with thermal imaging can detect movement in terrain inaccessible to ground patrols. Certain applications also incorporate AI-enabled analytics, allowing authorities to identify patterns suggesting smuggling networks or trafficking operations. Interoperable data systems can facilitate the sharing of intelligence between member states and regional bodies.

Evidence from recent deployments can be said to support some of these capabilities. South Africa's deployment of AI-powered drone surveillance along its borders yielded measurable results: during the 2025 Easter cross-border security operation — a coordinated holiday-period enforcement campaign conducted by the Border Management Authority at major ports of entry and land borders — 6,253 attempted irregular crossings were detected (3,841 more than the same period in 2024) (SAnews.gov.za 2025). Kenya has similarly emphasized the growing role of technology-enabled border management, including AI-supported surveillance and monitoring systems, as part of broader efforts to address evolving cross-border security threats.

Technical and Structural Risks

Yet these technologies carry significant risks that require systematic analysis. The technical risks are well documented: AI systems exhibit inherent algorithmic biases stemming from the composition of training data sets. Research consistently demonstrates that facial recognition systems perform less accurately on darker-skinned individuals (Buolamwini and Gebru 2018; Grother,

1 *OAU Convention Governing the Specific Aspects of Refugee Problems in Africa* [*OAU Refugee Convention*], 10 September 1969 (entered into force 20 January 1974), online: <https://au.int/sites/default/files/treaties/36400-treaty-36400-treaty-oau_convention_1963.pdf>.

2 *African Union Convention on Cyber Security and Personal Data Protection*, 27 June 2014 (entered into force 8 June 2023), online: <https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf>.

Ngan and Hanaoka 2019), a finding with obvious implications for African border deployments where such systems will disproportionately encounter the populations on which they perform the worst. The IOM has noted concerns about interoperable information technology (IT) systems that enable data to be easily shared across different systems, particularly regarding biometric data collection and cross-border data transfers (Beduschi and McAuliffe 2022).

The structural risks are equally significant. Data sovereignty remains critically weak across the continent, with Africa accounting for less than two percent of global data centre capacity, the majority of which is concentrated in South Africa (Africa Data Centres Association 2024). This creates dependency relationships wherein African states deploy technologies they cannot fully audit, maintain or control. When biometric border systems are provided by external vendors (whether European, Chinese or American), questions arise about who owns the data, where it is processed, under what legal frameworks it is protected and whether it may be shared with the vendors' home governments or other third parties.

The AU *Continental Artificial Intelligence Strategy* acknowledges these concerns, emphasizing that AI systems must be adapted to local realities, "considering African contexts, cultures and values" (African Union 2024, 4). It also highlights the importance of African control over data resources, calling for stronger continental data governance frameworks and investment in local data infrastructure to support digital sovereignty. The strategy further calls for developing "a legal framework to regulate digital platforms and protect African people from misuse" (ibid., 51). Yet implementation remains constrained by capacity gaps: analysis of 18-month implementation data (between July 2024 and October 2025) reveals stark geographic concentration, with 83 percent of AI start-up funding flowing to just four countries (Egypt, Kenya, Nigeria and South Africa), minimal private sector mobilization relative to estimated continental needs and AI governance frameworks that remain largely aspirational (Giacomelli 2026).

Refugee Protection and the Moral Dilemmas of Borders

The deployment of AI-driven border technologies directly intersects with the obligations of AU member states under international refugee law. The 1951 UN Refugee Convention[3] and the 1969 *OAU Refugee Convention*[4] establish binding commitments to provide international protection to persons fleeing persecution. The principle of non-refoulement (the prohibition on returning refugees to territories where their lives or freedom would be threatened) constitutes a cornerstone of both conventions.

Neither convention explicitly requires states parties to permit refugees to enter their territories. In practice, however, protection cannot operate unless people fleeing persecution are able to reach a place where they can request asylum. Without some form of territorial access, the refugee protection regime cannot function as intended. Refugees accessing the territories of states parties is a *sine qua non* for the objects and purposes of both instruments to be achieved. This creates what Rainer Bauböck, Julia Mourão Permoser and Martin Ruhs (2022) have termed "hard ethical dilemmas," or persistent conflicts between morally worthy goals, particularly between states' legitimate interest in controlling their borders and their obligation to ensure meaningful access to asylum and protection for those fleeing persecution; these dilemmas are embedded in political institutions and cannot be easily resolved.

AI-driven border technologies intensify these dilemmas. Perimeter intrusion detection systems, drone surveillance and predictive analytics do not distinguish between economic migrants seeking better opportunities and refugees fleeing persecution. Automated risk-scoring systems may flag individuals based on nationality, travel patterns or other proxies that correlate with refugee

3 *Convention Relating to the Status of Refugees*, 28 July 1951, 189 UNTS 137 (entered into force 22 April 1954) [*Refugee Convention*], online: <www.unhcr.org/media/1951-refugee-convention-and-1967-protocol-relating-status-refugees>.

4 *OAU Refugee Convention*, *supra* note 1.

populations. Biometric systems that capture data at informal crossing points may subsequently be used (often with human decision makers relying on or reviewing the outputs) to identify and return individuals who might otherwise have sought asylum. The technology, in other words, enables a form of "push back" at scale, one that occurs not through physical violence but through the algorithmic management of mobility itself.

Article 33(1) of the 1951 Refugee Convention exhorts states parties to abstain from expelling or returning a refugee "in any manner whatsoever" to territories where their life or freedom would be threatened.[5] The phrase "in any manner whatsoever" merits attention in the technological context. While traditionally interpreted to address physical deportation or interception at sea, the deployment of AI systems that systematically prevent refugees from accessing territorial protection may constitute constructive refoulement, achieving through technological means what would be prohibited if carried out by physical force.

Human rights advocates and UN bodies assert that the right of states to control their borders is not absolute. The 2016 New York Declaration for Refugees and Migrants reaffirmed member states' obligations to protect the human rights and fundamental freedoms of all refugees and migrants, regardless of status.[6] Yet these principles must be operationalized within systems where AI enables border enforcement at unprecedented scale and efficiency, systems that may render protection obligations effectively unenforceable without explicit technological carve outs for asylum procedures.

The Construction of Fortress Africa: Internal and External Dynamics

The spectre of "Fortress Europe" looms large in discussions of African border governance. Originally referring to Nazi Germany's defensive fortifications during the Second World War, the term now denotes the European Union's increasingly restrictive approach to migration and asylum, characterized by externalization, securitization and the deployment of surveillance technologies to prevent irregular arrivals (Widom 2022). The question is whether Africa is constructing its own fortress, and if so, who is building it.

The European Precedent

Europe's trajectory toward what is often described as Fortress Europe began with institutional arrangements framed as burden sharing. The 1990 Dublin Convention[7] and subsequent regulations assigned responsibility for asylum claims to the first EU member state of entry, concentrating pressures on frontline states and encouraging deterrence-oriented border management. These measures were reinforced by expanding surveillance infrastructure, including the Schengen Information System (SIS), Eurodac biometric databases and Frontex monitoring operations. More recent developments illustrate similar tensions. The EU AI Act, adopted in 2024, provides limited protections for non-citizens and exemptions for migration-related uses, while AI-enabled border screening and the growing interoperability of EU border databases coordinated through the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), including systems such as Eurodac and the SIS, continue to deepen technology-driven migration control at Europe's external borders.

5 *Refugee Convention, supra* note 3, art 33(1).

6 *New York Declaration for Refugees and Migrants*, GA Res 71/1, UNGAOR, 71st Sess, Supp No 1, UN Doc A/RES/71/1 (19 September 2016), online: <https://docs.un.org/en/A/RES/71/1>.

7 EC, *Convention determining the State responsible for examining applications for asylum lodged in one of the Member States of the European Communities*, [1997] OJ, C 254/1 [*Dublin Convention*], online: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A41997A0819%2801%29>.

Externalization as Construction

Critically, the construction of Fortress Europe is not confined to European territory. EU border externalization policies actively extend surveillance infrastructure into African states. Frontex's budget has expanded from approximately €143 million in 2015 to €922 million in 2024, surpassing €1 billion for the first time in 2025 (Frontex 2025; Statista Research Department 2026). The agency's presence in West Africa has grown through the establishment of risk analysis cells, which embed Frontex personnel within local border agencies, enabling real-time monitoring of migrant movements. Funded "capacity-building" programs provide surveillance technologies to partner states.

The European Union's Neighbourhood, Development and International Cooperation Instrument, with a total allocation of €79.5 billion, conditions development assistance on migration cooperation (European Commission 2021; Pope and Weisner 2023). This creates what might be termed "surveillance conditionality": African states receive technology, training and funding in exchange for participation in European border enforcement priorities. The results are documented: in May 2024, investigative journalists reported that in Mauritania, Morocco and Tunisia, migrants from Sub-Saharan Africa were rounded up and expelled to remote desert areas in operations intended to deter onward migration toward Europe. The reporting highlighted that those targeted were overwhelmingly Black Africans, reflecting the composition of the migrant population moving along these routes. Vehicles used in these operations were traced to European funding.

Biometric data collected through EU-funded programs flows into European databases. The MIDAS system in Nigeria, biometric registration in Mauritania and risk analysis cells across the Sahel all capture data that is shared with Europol and Frontex. This creates an asymmetric surveillance relationship: African migrants' biometric data is extracted in Africa, processed on European platforms and potentially used to facilitate their deportation if they later approach EU borders. The European Union's interoperable database architecture, coordinated through eu-LISA and supported by the European Border Surveillance System, links databases such as Eurodac, the Visa Information System, the SIS and the Entry/Exit System, enabling information collected at different stages of migration to contribute to shared situational awareness across the European Union's external border management network.

Internal AU Dynamics

The African Union does not yet possess a centralized refugee responsibility allocation system comparable to the Dublin regulation. Yet it can be argued that the building blocks exist. The AU border governance strategy (AU Commission 2020), migration frameworks (AU Commission 2006, 2018) and the African Continental Free Trade Area's (AfCFTA's)[8] provisions on free movement create an institutional architecture that, under pressure, could evolve toward exclusionary configurations. The AU *Continental Artificial Intelligence Strategy*'s implementation plan envisions harmonized national approaches and interoperable systems across member states.

Individual member-state deployments demonstrate this trajectory:

- Ghana's biometric border system connects identity verification to a broader e-governance infrastructure.
- Kenya's 2025 border strategy explicitly links drone surveillance, biometric systems and AI-powered analytics in an integrated border enforcement architecture.
- South Africa's deployment of AI-powered surveillance has been associated with reported increases in border interdictions and operational efficiency in border management.

The continental trajectory points toward an increasingly layered border surveillance architecture, not built by a single architect but constructed through the accumulation of bilateral arrangements, technology transfers, capacity-building programs and national deployments: each individually defensible, collectively creating a surveillance infrastructure that may prove difficult to dismantle once established. The "Fortress Africa" scenario, therefore, while still evolving, reflects a trajectory shaped by the cumulative effects of these technological deployments and institutional arrangements.

8 *Agreement Establishing the African Continental Free Trade Area*, 21 March 2018 (entered into force 30 May 2019), online: <https://au.int/sites/default/files/treaties/36437-treaty-consolidated_text_on_cfta_-_en.pdf>.

Recommendations: Toward a Rights-Based Framework for AI Border Governance

The African Union's existing legal and policy infrastructure provides foundations for a rights-based approach to AI border governance. The Malabo Convention, which entered into force in June 2023 after Mauritania became the fifteenth ratifying state, establishes general principles for data protection, including provisions on cross-border data transfers.[9] The AU *Data Policy Framework* provides guidance on data governance (African Union 2022), and the AU *Continental Artificial Intelligence Strategy* emphasizes ethical, responsible and equitable AI development (African Union 2024). Yet these frameworks remain only partially implemented in practice. Only 16 of the 55 AU member states have so far ratified the Malabo Convention (African Union 2024). Approximately 36 African countries have formal data protection regulations; however, implementation and enforcement vary significantly (Wanyama 2024). As of early 2026, at least 17 African states had adopted national AI strategies, with several others in draft stage, although capacity for implementation remains uneven (Organisation for Economic Cooperation and Development 2026). Fewer than 10 countries have drafted national AI strategies. The governance-capacity gap is stark: sophisticated normative frameworks coexist with severe implementation constraints stemming from infrastructure deficits, capacity limitations and resource scarcity.

A rights-based framework for AI border governance must address both the technical and structural dimensions of the challenge, including the following.

AIAs

AIAs must become mandatory prior to any AI border technology deployment. Such assessments must evaluate not only technical accuracy and bias but also structural impacts: how the technology affects access to asylum procedures, whether it creates systematic disadvantages for particular populations and how it interacts with existing surveillance infrastructure. AIAs should be conducted by independent bodies with technical expertise and human rights competence, with findings made publicly available. The African Union should develop a standardized AIA methodology tailored to African contexts and provide technical assistance to member states that lack assessment capacity.

Data Sovereignty and Localization

AU member states should require that biometric and surveillance data collected at African borders be stored and processed within Africa, where adequate legal safeguards and independent oversight are in place, ensuring that data governance aligns with African legal frameworks while avoiding undue concentration of sensitive data in jurisdictions with weak protections. This regulation would require investment in data centre infrastructure (a challenge given that only two percent of African data is currently stored in Africa), as well as assertive legal stipulations in technology-procurement contracts. Data-sharing agreements with external parties, including EU agencies, should be subject to rigorous conditions, including clear limits on how the data may be used, strict retention periods and prohibitions on secondary use for immigration enforcement outside Africa. The AfCFTA digital protocol provides a framework for operationalizing these requirements within broader continental integration.[10]

Refugee Protection Carve Outs

AI border systems must incorporate explicit procedural safeguards to ensure that automated detection and interdiction do not override access to asylum procedures. These safeguards might include:

- → mandatory human review of any AI-assisted interdiction decision;
- → prohibition on using AI risk scoring to deny access to asylum procedures;

9 *Dublin Convention, supra* note 7.

10 *Protocol to the Agreement Establishing the African Continental Free Trade Area on Digital Trade*, 18 February 2024 (not yet entered into force), online: <https://au.int/sites/default/files/treaties/45079-treaty-EN_AfCFTA_Protocol_on_Digital_Trade.pdf>.

- → requirements that automated systems flag rather than automatically deny entry to individuals who may qualify for protection; and
- → regular audits to assess whether AI deployments have reduced asylum claims in ways that suggest systematic denial of access.

Member states should consider whether AI-assisted pushbacks constitute constructive refoulement, which would require a legal prohibition.

Independent Oversight Mechanisms

Effective oversight requires institutional independence, technical competence and meaningful enforcement authority. National independent regulators (such as data protection authorities or dedicated digital governance bodies, supported by regional coordination through the African Union or sub-regional institutions) should have the power to audit AI systems, investigate complaints and order remediation of systems that violate rights standards. Critically, oversight must extend to agreements with external partners: EU-funded technology transfers, Frontex cooperation agreements and biometric data-sharing arrangements should all be subject to independent review. Civil society organizations and affected communities should have meaningful participation in oversight processes: not merely consultation but structural roles in governance bodies.

Transparency and Accountability

Member states should publicly disclose the AI systems deployed at their borders, the types of data collected, the processes by which decisions are made and the safeguards in place. Technology vendors should be required to provide sufficient documentation to enable independent auditing. Individuals affected by AI-driven border decisions should have the right to know what data-informed decisions are made about them and to challenge those decisions before human adjudicators. Aggregate statistics on AI-assisted interdictions, disaggregated by nationality and outcome, should be published on a regular basis.

Renegotiating External Relationships

AU member states and the AU Commission should collectively reassess border cooperation arrangements with external partners, particularly the European Union. Agreements that condition development assistance on migration enforcement, require the sharing of biometric data with European agencies or fund surveillance infrastructure serving primarily European deterrence objectives should be renegotiated to ensure that they align with African development priorities. Where externally funded systems cannot be brought into compliance with African rights frameworks, termination should be considered. The African Union should develop model agreements for border technology cooperation that preserve African data sovereignty and refugee protection commitments.

Conclusion

AI-driven border technologies present both opportunities and dangers for AU member states. The security rationale is genuine: porous borders, limited enforcement capacity and serious transnational threats warrant technological innovation. Yet the manner in which these technologies are deployed, governed and integrated into broader surveillance architectures will determine whether they serve African development priorities or perpetuate neo-colonial patterns of extraction and control. The Fortress Africa scenario is not merely hypothetical as the building blocks are already in place: EU-funded surveillance infrastructure across the Sahel and West Africa; biometric databases capturing African migrants' data for European platforms; and member-state deployments that prioritize interdiction over protection. Without deliberate intervention, the accumulation of these elements will produce continental fortress dynamics, not through any single policy choice but through the gradual normalization of surveillance as the dominant modality of border governance. The AU *Continental Artificial Intelligence Strategy* offers a framework for a distinct trajectory, one rooted in African values, responsive to African contexts and focused on inclusive development. Realizing this vision requires not only technical capacity but also political will: the will to assert data sovereignty against external pressures, to prioritize refugee protection alongside security and to subject AI deployments to meaningful rights-based oversight. Africa's long-standing commitment to refugee protection, exemplified in the 1969 OAU Refugee Convention and in the continent's hosting of some of the world's largest refugee populations

despite limited resources, represents a distinctive contribution to international human rights. AI-driven border technologies need not undermine this commitment but they will unless governance frameworks are designed to prevent these technologies from restricting access to asylum and refugee protection. The choice is not between security and rights but between surveillance regimes shaped primarily by external migration-control priorities and rights-respecting systems that serve the interests of African peoples.

Acronyms and Abbreviations

AfCFTA	African Continental Free Trade Area
AI	artificial intelligence
AIAs	algorithmic impact assessments
AU	African Union
eu-LISA	European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice
IOM	International Organization for Migration
IT	information technology
MIDAS	Migration Information Data Analysis System
OAU	Organisation of African Unity
SIS	Schengen Information System

Works Cited

Africa Data Centres Association. 2024. *Data Centres in Africa Focus Report 2024*. https://africadca.org/en/data-centres-in-africa-focus-report-2024.

African Union. 2022. *AU Data Policy Framework*. February. https://au.int/sites/default/files/documents/42078-doc-DATA-POLICY-FRAMEWORKS-2024-ENG-V2.pdf.

— — —. 2024. *Continental Artificial Intelligence Strategy: Harnessing AI for Africa's Development and Prosperity*. July. https://au.int/sites/default/files/documents/44004-doc-EN-_Continental_AI_Strategy_July_2024.pdf.

AU Commission. 2006. *The Migration Policy Framework for Africa*. Addis Ababa, Ethiopia: African Union Commission. https://au.int/sites/default/files/pages/32899-file-1._au_migration_policy_framework_for_africa.pdf.

— — —. 2018. *Migration Policy Framework for Africa and Plan of Action (2018–2030)*. May. Addis Ababa, Ethiopia: African Union Commission. https://au.int/sites/default/files/documents/35956-doc-2018_mpfa_english_version.pdf.

— — —. 2020. *African Union Strategy for a Better Integrated Border Governance*. Addis Ababa, Ethiopia: African Union Commission. June. www.peaceau.org/uploads/2020-english-au-border-governance-strategy-final.pdf.

Bauböck, Rainer, Julia Mourão Permoser and Martin Ruhs. 2022. "The ethics of migration policy dilemmas." *Migration Studies* 10 (3): 427–41. https://doi.org/10.1093/migration/mnac029.

Beduschi, Ana and Marie McAuliffe. 2022. "Artificial Intelligence, Migration and Mobility: Implications for Policy and Practice." In *World Migration Report 2022*, edited by Marie McAuliffe and Anna Triandafyllidou. Geneva, Switzerland: IOM. https://publications.iom.int/system/files/pdf/WMR-2022-EN-CH-11.pdf.

Bulman, May, Maud Jullien, Tomas Statius, Monica C. Camacho, Beatriz Ramalho da Silva, Jack Sapoch, Klaas van Dijken, Eman El-Sherbiny, Andrei Popoviciu, Halima Salat Barre et al. 2024. "Desert Dumps." Lighthouse Reports, May 21. www.lighthousereports.com/investigation/desert-dumps/.

Buolamwini, Joy and Timnit Gebru. 2018. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification." *Proceedings of Machine Learning Research* 81: 77–91. https://proceedings.mlr.press/v81/buolamwini18a.html.

European Commission. 2021. "European Commission welcomes the endorsement of the new €79.5 billion NDICI-Global Europe instrument to support EU's external action." News Article, March 19. https://neighbourhood-enlargement.ec.europa.eu/news/european-commission-welcomes-endorsement-new-eu795-billion-ndici-global-europe-instrument-support-2021-03-19_en.

Frontex. 2025. *Consolidated Annual Activity Report 2024*. September. Warsaw, Poland: European Border and Coast Guard Agency. www.frontex.europa.eu/assets/Publications/General/CAAR_2024_Official_Publication.pdf.

Giacomelli, Max Cuvellier. 2026. "Where are the investors?" *Africa: The Big Deal* (blog), May 12. https://thebigdeal.substack.com/p/invest426?utm_campaign=post-expanded-share&utm_medium=web&triedRedirect=true.

Glover, Barbara, Bhekani Mbuli and Chifundo Kungade. 2021. "Enhancing Border Security In Africa Using Smart Border Control Technologies." *African Union Development Agency–New Partnership for Africa's Development* (blog), October 5. www.nepad.org/blog/enhancing-border-security-africa-using-smart-border-control-technologies.

Grother, Patrick, Mei Ngan and Kayee Hanaoka. 2019. *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*. NISTIR 8280. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8280.

Organisation for Economic Cooperation and Development. 2026. *AI governance in Africa: Insights from a policy dialogue with 12 countries*. OECD Case Study, April. 30. www.oecd.org/content/dam/oecd/en/publications/reports/2026/04/oecd-artificial-intelligence-case-studies_71322177/strengthening-ai-governance-in-africa_812bb149/1ff55135-en.pdf.

Pope, Stephanie and Zina Weisner. 2023. *From Development to Deterrence? Migration spending under the EU Neighbourhood, Development and International Cooperation Instrument (NDICI)*. Oxfam Briefing Paper. September. Oxford, UK: Oxfam Policy and Practice. https://doi.org/10.21201/2023.621536.

SAnews.gov.za. 2025. "BMA Easter ops turn the tide on illegal border crossings." South African Government News Agency, April 29. www.sanews.gov.za/south-africa/bma-easter-ops-turn-tide-illegal-border-crossings.

Statista Research Department. 2026. "Annual budget of Frontex in the European Union from 2005 to 2024." Statista, March 9. www.statista.com/statistics/973052/annual-budget-frontex-eu/.

Wanyama, Edrine. 2024. "The Impact of Artificial Intelligence on Data Protection and Privacy in Africa." *Collaboration on International ICT Policy for East and Southern Africa* (blog), May 29. https://cipesa.org/2024/05/the-impact-of-artificial-intelligence-on-data-protection-and-privacy-in-africa/.

Widom, Haley. 2022. "Fortress Europe." American University School of International Service, Transatlantic Policy Center, April 12. www.american.edu/sis/centers/transatlantic-policy/20220412-fortress-europe.cfm.

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

Director, Program Management Dianna English
Senior Program Manager Ifeoluwa Olorunnipa
Publications Editor Christine Robertson
Graphic Designer Abhilasha Dewan

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
cigionline.org

CIGI