Africa's Expansion of AI Surveillance — Regional Gaps and Key Trends

- **AI surveillance is still an emerging trend in Africa but already many governments and companies are implementing facial recognition systems, safe city projects, cloud computing infrastructures, and smart policing initiatives.**
- **AI surveillance tools have the potential to exacerbate existing inequalities if not deployed with proper governance mechanisms and adequate safeguards.**
- **AI surveillance use in Africa is not transparent. Surveillance technologies are not transparently procured or operated, and emphasis is placed on security or smartness of technology, without any risk mitigation frameworks in place to protect people's rights particularly safeguarding their data.**

Introduction

Many African states are deploying Artificial Intelligence (AI) surveillance technologies to monitor citizens for various purposes, but seldom in ways that are rights-respecting and particularly privacy-respecting. Today's AI surveillance technologies are capable of analysing big data, monitoring and tracking by classifying people's movements into astonishingly precise categories (Feldstein, 2019). These AI-powered tools provide governments and companies with the capability to gather and freely access personal data, which may cause serious harms (Stoycheff et al., 2019).

Africa needs to progress towards a world of AI that improves the delivery of public services and public goods rather than cause harm to society.

As AI increasingly moves towards becoming a general-purpose technology, Africa needs to develop governance frameworks that enable the delivery of public services and public goods while preventing harms and mitigating risks. For instance, in the wake of the COVID-19 pandemic AI powered by data science and machine learning is being applied in many areas, including in drug discovery (Zhou et al., 2020) as well as in public health management and public policy to model and predict outbreaks and COVID spread and help with contact tracing (Bragazzi et al., 2020). As AI is increasingly being used to tackle national and global problems like the COVID-19 pandemic, governments are increasingly adopting measures that can lead to violations of human rights. This raises the challenge of preserving and upholding both individual and collective rights.

AI is a set of theories, approaches, methods and applications – such as machine learning, deep learning and neural networks – increasingly used in many aspects of computing and everyday life. The International Development Research Centre (IDRC) defines AI as "an area of computer science devoted to developing systems that can be taught (e.g., through encoding expert knowledge) or systems that can learn (from data) to make decisions and/or predictions within specific contexts" (Smith & Neupane, 2018). AI often combines machine learning and data analytics to assist with decision-making.

Globally, the applications of AI are proliferating faster than individuals' abilities to opt-in or out of their data being processed by AI. As companies are gaining insights into people through their data, they are also able to influence people's choices with this data. Evidence shows how deeply polarised, and abusive AI systems powered platforms are to users (DiResta, 2018). AI is also starting to change government's approach and attitude to delivering public services.

Research ICT Africa is carrying out a mapping exercise, gathering empirical data on computer vision and surveillance across 14 countries in Africa. In so doing, our purpose is to facilitate evidence-based and informed policymaking in the context of emerging surveillance systems that are changing the ability of states and corporations to monitor citizens. The study has preliminarily identified a range of deployments, from facial recognition systems, safe city projects and cloud computing infrastructures, to smart policing initiatives that are meant to achieve various goals.

Potential Risks and Harms — How can we ensure Responsible AI?

Though state surveillance is not necessarily unlawful, it can be harmful when deployed in contexts of political repression that limit or restrict individual rights and freedoms. There can be legitimate justifications (such as in combatting threats to the public order or to safety) for undertaking mass or targeted surveillance. In addition, surveillance activities need to conform to "necessity and proportionality", global standards which limit surveillance to circumstances that are "strictly and demonstrably necessary to achieve a legitimate aim".[1] The lack of transparency by private companies doing business with states to supply AI surveillance tools, also present risks such as surveillance being used to achieve political agendas or to silence critics. In addition, there are significant novel interferences with user privacy and data exploitation by private companies.

Surveillance activities need to conform to "necessity and proportionality", global standards which limit surveillance to circumstances that are "strictly and demonstrably necessary to achieve a legitimate aim".

We list surveillance initiatives in each country according to who the key partners and controlling entities are. However, we also look at oversight mechanisms such as AI governance structures, freedom of expression and data privacy. These factors can be assessed to analyse the potential human rights implications of AI surveillance in specific countries. We ask important questions about the mitigation of the risks and harms of AI surveillance such as: Which African countries currently have data protection laws? Are there immediate data governance priorities to ensure a foundation for responsible use of AI surveillance technologies in Africa? And what policy interventions might assist in advancing inclusive, controllable, and trustworthy AI surveillance in the region?

Common Trends

Although the mapping data does not provide a comprehensive picture of what is happening everywhere in Africa, it is evident that AI surveillance is an emerging issue in the region. In general, the Sub-Saharan Africa AI surveillance landscape does not provide a

[1] See Electronic Frontier Foundation and a coalition of NGOs, '*Necessary & Proportionate Principles on Application of Human Rights to Communications Surveillance*', available at https://necessaryandproportionate.org/principles/#the-principles

clear picture of the adoption of AI surveillance tools, even the uptake of these tools is somehow slower. This is likely due to inadequate technological infrastructure to support AI readiness (Oxford Insights, 2020). Most African countries are still struggling to deliver broadband access to their populations, with levels remaining below 20% of the critical mass to enjoy its network effects (Gillwald et al., 2016). However, given the market-driven approach and persuasiveness of companies towards state entities driving the deployment of AI surveillance in Africa, the rate of adoption is likely to increase progressively. A key challenge in identifying the incidence of AI surveillance in Africa is that governments especially rarely disclose their surveillance practices or technologies, and the definitions of surveillance approaches often lack sufficient clarity to distinguish when and how AI plays a role.

To develop complex AI systems, vast amounts of data is needed. Many AI systems are currently developed through invasive techniques to collect people's personal data. Many AI systems collect vast amounts of data and apply invasive techniques to utilise personal data which benefits private companies. There is extensive involvement of private sector entities in driving the deployment of AI systems. Smart city/safe city initiatives are emerging across 14 countries mapped through public-private partnerships between state and technology companies in countries such as in Kenya, Ivory Coast and Botswana; while others appear to be listed as public safety initiatives meant to enhance security in public areas in countries such as Algeria and South Africa. Some countries, such as Kenya (Konza Data Center) and Egypt (Cloud Data Platform) have proposed cloud servers to support major smart city projects. Although cloud computing may not be categorised as a surveillance technology, it is important to note that it acts as an enabler of, and may support surveillance technologies.

The use of facial recognition technology is proliferating at a rapid rate, faster than measures ensuring that people's rights are protected in its deployment. Legislation and regulation of facial recognition is however slowly starting to respond. Californian legislators, for example, recently passed a bill that bans the use of facial recognition technology by police, which could potentially develop an overly oppressive surveillance state (Conger et al., 2019). Facial recognition is often deployed at countries' main points of entry for immigration purposes, such as airports and border posts. Initiatives in the smart policing category tend to be deployed with the intended purpose of facilitating investigations and police response to public crime where data-driven command centres are established to analyse the data collected. It is unclear whether these centres incorporate automated decision-making and algorithmic analysis to make predictions about crimes. There are, however, privacy and human rights concerns regarding the way data is gathered and processed by AI systems. These initiatives have the potential to cause harms in the absence of data protection frameworks that regulate how AI systems can process personal data.

Regional Differences

While the AI surveillance initiatives we found do not provide a comprehensive scan of the AI surveillance landscape in Africa they do reveal some interesting developments in how various states are adopting AI surveillance technologies. The initiatives were categorized as either: i) facial recognition (in eight countries), ii) smart city/safe city (in seven countries) or iii) smart policing (in six countries).

Out of the fourteen countries mapped, Southern Africa was ahead of the other regions with a total of six countries registered followed by three in East Africa, three in North Africa and two in West Africa.

Not all countries have data protection laws in place and enforced, which could help to protect people from the harmful effects of AI surveillance. Zimbabwe, Botswana, and Zambia have data protection laws which are either in the process of being developed or enacted without enforcement, while Namibia does not have any existing laws. In East Africa, Uganda and Kenya have not yet enforced any data protection laws, while Rwanda does not have any laws in place. Most countries mapped in West and North African regions, including Nigeria and Ghana, have data protection laws enforced except for Egypt.

We identified safe city/smart city surveillance initiatives emerging significantly that transmit real-time data to facilitate public safety in countries like Algeria, Kenya, Botswana and South Africa.

Despite this, in the African region, there appears to be an imbalance in policy development on AI national strategies with some initiatives lacking consideration of the local context. For example, some important lessons for South Africa from other country cases is that developing regulatory frameworks, to ensure ethical use of AI and considering 'cultural aspects' of the internet helps create a dynamic policy space that supports companies and government to enforce ethical and transparent use of AI technologies. This is a benchmark from Japan, where a High-Level Expert Group on Artificial intelligence (AI HLEG) has been established to "Draft Ethics Guidelines for Trustworthy AI") (Stella, 2020, p. 17).

The Western Cape province has also begun drafting legislation to govern the use of CCTV surveillance (IOL, 2020). Some countries like Kenya[2] and Mauritius[3] in the region have AI national strategies in place, which establishes ethics for the use of AI surveillance, for instance, the Mauritius' AI strategy action plan notes that "AI ecosystem should be ethical, and therefore, a permanent committee on ethics should be set up to maintain the dialogue and formulate proposals to maintain a healthy relationship between AI and humans". This is perhaps not surprising as Mauritius has shown leadership on the continent in relation to cyber policy, aligning itself with international normative frameworks on cybersecurity and data protection (Spuy et al., 2018).

Key Takeaways

- Technology firms are at the forefront of developing AI for states. While enabling AI innovation and application to private sector delivery and economic development in Sub-Saharan Africa, states should not abdicate their responsibilities to prevent harms and safeguard their citizens. There is increasing evidence of the potential risks and harms of AI, including algorithmic bias, transparency and accountability (Hoffmann,

[2] See the Kenyan Blockchain & Artificial Intelligence task force, provides a snapshot summary of some previous and ongoing initiatives, available at: https://kenyanwallstreet.com/kenya-govt-unveils-11-member-blockchain-ai-taskforce-headed-by-bitange-ndemo/

[3] See Mauritius Artificial Intelligence Strategy, available at: https://cib.govmu.org/Documents/Strategies/Mauritius%20AI%20Strategy%20(7).pdf2021/01/20 1:50:00 PM

2019). Therefore, Africa needs policies to govern private-sector usage and development of AI to ensure it is rights preserving and ethical in its design.

- The use of AI surveillance in the public sector should be transparent and regulated. Furthermore, as technological innovations continue to impact citizens' lives it is crucial to develop policy on how we monitor and govern public-private sector AI collaborations. Government and the private sector need to collaborate more with other stakeholders in finding solutions to the regulation of AI.
- As we continue to highlight emerging trends, we need to develop global standards, checks and balances that ensure transparency and accountability in the deployment of AI technologies, particularly surveillance technologies. While the development of domestic policies and governance framework is essential to safeguarding the rights of citizens in the global market, it raises jurisdictional issues, which will require global cooperation to address.

_____

Sign up to RIA's newsletter here. Find more RIA policy briefs here.

Author

Oarabile Mudongo

omudongo@researchictafrica.net

Enquiries

info@researchictafrica.net

T: +27 214476332

W: www.researchictafrica.net

References

Conger, K., Fausset, R., & Kovaleski, S. F. (2019, May 14). San Francisco Bans Facial Recognition Technology (Published 2019). *The New York Times*. https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

DiResta, R. (2018, November 4). The Web's Recommendation Engines Are Broken. Can We Fix Them? *Wired*. https://www.wired.com/story/creating-ethical-recommendation-engines/

Feldstein, S. (2019). *The Global Expansion of AI Surveillance*. The Carnegie Endowment for International Peace. https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf

Gillwald, A., Odufuwa, F., Rademan, B., & Esselaar, S. (2016). *An Evaluation Of Open Access Broadband Networks In Africa: The Cases Of Nigeria And South Africa* (Policy Paper Series 4: Broadband for Africa). https://researchictafrica.net/publications/Other_publications/2016_Integrated_Policy_Paper_-_Open_Access_Broadband_Networks_in_Africa.pdf

Hoffmann, A. L. (2019). Where fairness fails: Data, algorithms, and the limits of antidiscrimination discourse. *Information, Communication & Society*, 22(7), 900–915. https://doi.org/10.1080/1369118X.2019.1573912

IOL. (2020). Cape to be first with CCTV law. https://www.iol.co.za/weekend-argus/news/cape-to-be-first-with-cctv-law-5eec5881-c3a8-40f7-8397-b79d65452de0

Oxford Insights. (2020). Government AI Readiness Index 2020—Oxford Insights. Oxford Insights.https://www.oxfordinsights.com/government-ai-readiness-index-2020

Smith, M. L., & Neupane, S. (2018). *Artificial Intelligence and Human Development: Towards a Research Agenda* (p. 25). International Development Research Centre. https://www.idrc.ca/sites/default/files/ai_en.pdf

Stoycheff, E., Liu, J., Xu, K., & Wibowo, K. (2019). Privacy and the Panopticon: Online mass surveillance's deterrence and chilling effects. *New Media & Society*, *21*(3), 602–619. https://doi.org/10.1177/1461444818801317

Smith, M. L., & Neupane, S. (2018). Artificial Intelligence and Human Development: Towards a Research Agenda (p. 25). International Development Research Centre. https://www.idrc.ca/sites/default/files/ai_en.pdf

Spuy, A. V. D., Calandro, E., Brown, I., & Oolun, K. (2018). Collaborative Cybersecurity: The Mauritius Case (Africa Digital Policy) [Policy Brief]. Research ICT Africa. https://researchictafrica.net/wp/wp-content/uploads/2018/11/Policy-Brief-ADPP-N-1-Collaborative-Cybersecurity-Mauritius-Case.pdf

Zhou, Y., Wang, F., Tang, J., Nussinov, R., & Cheng, F. (2020). Artificial intelligence in COVID-19 drug repurposing. *The Lancet Digital Health*, 2(12), e667–e676. https://doi.org/10.1016/S2589-7500(20)30192-8