

ARTIFICIAL INTELLIGENCE AND NATIONAL SECURITY: ETHICAL IMPLICATIONS OF ARTIFICIAL INTELLIGENCE SURVEILLANCE IN COUNTERTERRORISM OPERATIONS IN NIGERIA

Solomon Kumapayi PhD

08032165765

[sbabatunde152@gmail.com](mailto:sbatunde152@gmail.com)

International Academy for Gender and Peace

Abstract

The world is rapidly searching for the easiest and fastest ways of resolving human-made and natural disaster around the globe. The advent of Artificial Intelligence has remarkably appeared on world stage as the most effective tool for human beings to improve their living condition without depending on existing traditions. The challenge facing the use of Artificial Intelligence in contemporary society is the speed at which its development is moving across the globe. It is becoming extremely difficult to catch up with the trend, not to talk of controlling it. Artificial Intelligence has contributed immensely to improvement of health, education, climate change, transportation, security. These good things of life are punctuated by heavily observed ills as a result of the usage of AI. Counterterrorism operations in Nigeria is expected to put an end to presence of terrorism, banditry, kidnapping, but the unethical practices surrounding the use of AI has made it very difficult for government to win the battle against the non-state actors, ethnic militia and

Introduction

Artificial Intelligence (AI) has become a defining element of contemporary national security architectures worldwide. In Africa, where terrorism, insurgency, and transnational crime continue to pose existential threats, governments are increasingly integrating AI-driven surveillance systems to enhance operational effectiveness. From facial recognition to predictive policing, AI technologies enable security institutions to gather, analyse, and act on vast amounts of data faster than human capability allows. While these innovations offer strategic advantages in counterterrorism, they also introduce complex ethical questions regarding privacy, oversight, and the limits of state power (Amoore, 2020).

The application of AI surveillance in counterterrorism operations is not merely a technological advancement; it represents a paradigm shift in how African states conceptualize and execute national security. Traditional methods of intelligence gathering are being complemented by algorithmic tools capable of identifying behavioural patterns and detecting anomalies within social and digital ecosystems. These systems promise greater precision and efficiency, yet they often operate in legal and ethical grey zones, particularly in contexts with weak data protection laws or limited judicial oversight (Abebe, 2022).

Africa's evolving security landscape marked by groups such as Boko Haram, Al-Shabaab, and ISIS affiliates demands adaptive and intelligent responses. AI surveillance technologies have been deployed to monitor social media communications, analyse satellite imagery, and track the movements of suspected militants. However, the moral and legal legitimacy of these surveillance activities remains contested, especially when they infringe upon citizens' rights to privacy and freedom of expression. The dilemma lies in balancing national security imperatives with ethical and human rights considerations (UNESCO, 2021).

Furthermore, the growing involvement of external actors, including Chinese and Western technology firms, in supplying AI surveillance infrastructure to African states introduces additional ethical complexities. Issues of data sovereignty, algorithmic bias, and dependency on foreign technology providers compound the challenges of ensuring accountability and transparency. Many African countries lack robust institutional frameworks to regulate the deployment and use of AI in security operations, resulting in a potential erosion of public trust (Mhlambi & Tiribelli, 2022).

This paper explores the ethical implications of AI surveillance in counterterrorism operations in Africa, emphasizing its intersections with national security, human rights, and technological governance. It begins with conceptual clarifications of key terms artificial intelligence, national security, AI surveillance, and counterterrorism operations followed by an overview of AI applications in African counterterrorism contexts. The discussion then examines key ethical implications, identifies prevailing challenges, and proposes strategic pathways for the ethical use of AI in safeguarding African societies. The analysis ultimately underscores that the pursuit of national security through AI must not come at the expense of the moral and democratic values that sustain it.

Artificial Intelligence (AI)

Artificial Intelligence refers to the simulation of human cognitive functions such as learning, reasoning, problem-solving, and perception by computer systems (Russell & Norvig, 2021). AI systems analyse large datasets, identify patterns, and make autonomous or semi-autonomous decisions that mimic aspects of human intelligence. In security contexts, AI applications include facial recognition, voice analysis, behavioural prediction, and autonomous surveillance. These systems are capable of processing complex data in real time, thereby enabling faster decision-making during counterterrorism operations. According to the African Union (2022), AI has emerged as a strategic enabler of national resilience and operational precision, but its integration raises profound ethical and legal concerns.

National Security

National security encompasses the protection of a nation's sovereignty, territorial integrity, institutions, and citizens from internal and external threats (Baldwin, 1997). It extends beyond military defence to include economic stability, political integrity, cyber defence, and the protection of critical infrastructures. In the African context, national security often revolves around addressing terrorism, insurgency, and transnational crime, which threaten political

stability and human development. Governments therefore justify surveillance activities and data monitoring as essential tools for preserving national security. However, ethical questions arise when such surveillance infringes on civil liberties and the democratic principles that underpin societal stability (Acharya, 2020).

Artificial Intelligence Surveillance

AI surveillance refers to the use of AI technologies to collect, process, and interpret data for monitoring human behaviour and environmental conditions (Wright & Kreissl, 2014). These systems utilize facial recognition, biometric identification, geospatial tracking, and predictive analytics to enhance situational awareness and threat detection. In counterterrorism operations, AI surveillance helps identify suspects, monitor digital communication networks, and anticipate potential attacks. While these capabilities improve operational effectiveness, they also risk enabling mass surveillance, data misuse, and discrimination. The ethical debate centres on how to regulate AI surveillance to prevent abuse and ensure respect for human rights (Fazlioglu, 2021).

Counterterrorism Operations

Counterterrorism operations involve coordinated military, intelligence, and law enforcement activities aimed at preventing, mitigating, and responding to acts of terrorism (Crenshaw, 2011). These operations require intelligence gathering, threat analysis, and rapid response strategies. In Africa, counterterrorism efforts target organizations such as Boko Haram in Nigeria, Al-Shabaab in Somalia, and ISIS affiliates in the Sahel. AI technologies support these efforts by enhancing intelligence fusion, improving border monitoring, and predicting insurgent movements. Nevertheless, the operational use of AI in such contexts must adhere to ethical standards and legal frameworks to avoid human rights violations and potential misuse of state power (Akinola, 2023).

Artificial Intelligence (AI) Surveillance on Counterterrorism Operations

AI surveillance has gained momentum as African states confront increasingly sophisticated terrorist networks. Governments have invested in digital surveillance systems, drones, and biometric databases to monitor potential threats. For instance, Nigeria's military and intelligence agencies utilize AI-assisted image recognition systems to identify Boko Haram hideouts, while Kenya employs predictive analytics for urban security management. These technologies enhance situational awareness and facilitate rapid responses to emerging threats (Ezeani, 2021).

International partnerships have also accelerated the adoption of AI surveillance. African governments collaborate with technology firms and foreign powers to develop integrated intelligence platforms. China's Huawei and ZTE have supplied "Safe City" AI systems to several African nations, including Ethiopia, Kenya, and Uganda (Feldstein, 2019). While these systems improve public safety, they raise concerns about data privacy, external influence, and potential political misuse against opposition groups and civil society actors.

AI surveillance systems are particularly effective in analysing open-source intelligence

and social media activities. Extremist organizations often exploit online spaces to recruit, radicalize, and coordinate attacks. Through natural language processing and sentiment analysis, AI tools can detect extremist content and predict radicalization patterns (UNDP, 2022). However, without clear ethical guidelines, these systems risk misidentifying innocent individuals or suppressing legitimate political expression, thereby undermining democratic freedoms.

In regions like the Sahel, AI technologies are being used to strengthen intelligence-sharing among joint task forces such as the G5 Sahel. Data fusion centres integrate information from drones, satellites, and human intelligence to enhance threat prediction. Nonetheless, the absence of harmonized legal frameworks across African states creates regulatory fragmentation, leaving citizens vulnerable to privacy breaches and surveillance abuses (Mhlambi & Tiribelli, 2022).

Despite these advances, Africa's AI surveillance landscape remains uneven. While some countries have adopted emerging technologies, others face infrastructural and capacity-related challenges. Moreover, ethical considerations such as consent, transparency, and accountability are often neglected. This imbalance calls for a pan-African approach to AI ethics, grounded in principles of human dignity, justice, and democratic governance. Without such frameworks, the region risks adopting AI in ways that perpetuate inequality and erode public trust in state institutions.

Challenges AI Surveillance faces during Counterterrorism Operations

This paper has identified four challenges facing Artificial Intelligence surveillance during Counterterrorism operations to include; weak legal and institutional frameworks, Limited Technical Expertise and Infrastructure, Limited Technical Expertise and Infrastructure, Potential for Human Rights Violations and Ethical and Cultural Contextualization. Each of the challenges is explained below.

Weak Legal and Institutional Frameworks

A primary challenge confronting AI surveillance in Africa is the absence of comprehensive legal and institutional frameworks to regulate its deployment. Many African countries have yet to establish robust data protection, cybersecurity, or AI-specific laws (African Union, 2022). Consequently, AI systems are introduced into counterterrorism operations without adequate oversight or ethical guidelines. This legal vacuum creates opportunities for arbitrary surveillance and the misuse of data under the pretext of national security. The lack of transparency also makes it difficult for citizens to know how their data are collected, stored, or used.

In addition, institutional capacity to enforce existing legal provisions is often weak. Regulatory bodies are underfunded or politically constrained, leaving them unable to monitor security agencies effectively. Without independent oversight mechanisms, governments may deploy AI tools beyond their intended purpose such as monitoring political opponents or suppressing dissent. Strengthening institutional capacity and enacting regionally harmonized AI

governance frameworks are essential to ensuring that AI surveillance adheres to ethical and democratic standards (Mhlambi & Tiribelli, 2022).

Limited Technical Expertise and Infrastructure

Another major obstacle is the scarcity of technical expertise and inadequate digital infrastructure across much of Africa. Deploying AI surveillance requires skilled personnel in data science, cybersecurity, and machine learning. However, many African security institutions lack the technical know-how to develop or manage AI systems internally (Ezeani, 2021). This dependence on foreign technology vendors increases vulnerability to external manipulation, data breaches, and cyber espionage. Moreover, most countries lack the computational resources and broadband infrastructure necessary for large-scale AI deployment.

This technological deficit perpetuates dependency on external actors, raising concerns about data sovereignty and ethical autonomy. Foreign companies providing AI solutions may not align with local ethical standards, thereby imposing external norms on African security operations. Bridging this gap requires significant investment in AI education, research, and infrastructure development to build indigenous capacity for ethical innovation and technological sovereignty (Akinola, 2023).

Potential for Human Rights Violations

AI surveillance in counterterrorism often intersects with human rights concerns. The broad powers granted to security agencies can lead to arbitrary arrests, unlawful data collection, and suppression of legitimate expression (UNESCO, 2021). In environments where democratic institutions are fragile, surveillance technologies can be weaponized against journalists, activists, and opposition figures. This erodes public trust and undermines the legitimacy of counterterrorism operations, as citizens begin to associate AI with state repression rather than protection.

Ethically, this challenge questions the compatibility of AI surveillance with fundamental human rights principles. Unchecked data collection and monitoring practices violate privacy, freedom of speech, and the right to due process. African governments must therefore ensure that AI applications in counterterrorism are bound by constitutional safeguards, judicial oversight, and adherence to international human rights standards such as the African Charter on Human and Peoples' Rights (1981). Failure to do so risks transforming counterterrorism into a tool of authoritarian control rather than public security.

Ethical and Cultural Contextualization

A further challenge lies in the insufficient ethical and cultural contextualization of AI in African societies. Most ethical frameworks guiding AI development are imported from Western contexts and may not reflect African values, communal norms, or socio-political realities (Mhlambi, 2020). This epistemic imbalance limits Africa's ability to define its ethical priorities in relation to surveillance, privacy, and accountability. For example, African societies often emphasize collective security and community wellbeing, which may sometimes conflict with Western notions of individual privacy.

The absence of localized ethical guidelines allows governments to adopt foreign AI systems without adapting them to local contexts. This can result in ethical dissonance and unintended consequences. Addressing this challenge requires the development of Afrocentric AI ethics frameworks that harmonize technological innovation with indigenous values such as Ubuntu emphasizing humanity, community, and mutual respect. Such frameworks would help ensure that AI surveillance aligns with Africa's unique cultural and moral foundations while safeguarding human dignity.

Ethical Implications of AI Surveillance in Counterterrorism Operations

There are numerous ethical implications of Artificial Intelligence encountered in counterterrorism operations that are worth considering in a study of this nature. Three critical implications are; ethics of privacy and data protection, algorithmic bias and discrimination, accountability and oversight. A brief discussion that brings out the ethical connotations is carried out below.

Ethics of Privacy and Data Protection

The most immediate ethical implication of AI surveillance lies in its intrusion into individual privacy. AI systems collect and analyse vast amounts of personal data, including biometric identifiers, movement patterns, and digital communications. In many African countries, data protection laws are either weak or poorly enforced, creating opportunities for abuse (Fazlioglu, 2021). The absence of explicit consent mechanisms violates fundamental human rights principles enshrined in the African Charter on Human and Peoples' Rights. Furthermore, indiscriminate data collection under the guise of counterterrorism undermines citizens' trust in government institutions.

Beyond the invasion of privacy, AI surveillance systems risk creating permanent databases that can be repurposed for political repression. For example, surveillance technologies initially deployed to combat terrorism have been used to monitor journalists and political opponents in some African countries (Feldstein, 2019). The ethical dilemma arises when governments exploit AI's capabilities to expand their control beyond legitimate security objectives. Protecting privacy, therefore, requires institutional safeguards and independent oversight mechanisms to ensure proportionality and accountability in surveillance activities.

Algorithmic Bias and Discrimination

AI systems are only as impartial as the data and algorithms that power them. When training data reflect existing social or ethnic biases, AI surveillance can reinforce discrimination and marginalization. In Africa, where data infrastructures are fragmented and often imported, AI models may misclassify individuals based on racial, ethnic, or socio-economic attributes (Abebe, 2022). This not only compromises the fairness of counterterrorism operations but also risks criminalizing specific communities.

Ethically, algorithmic bias challenges the principle of justice and equality before the law. When AI surveillance disproportionately targets minority groups, it erodes social cohesion and delegitimizes counterterrorism initiatives. To mitigate bias, African governments must prioritize inclusive data governance and develop localized AI models that reflect regional diversity. Establishing ethical review boards and mandating algorithmic transparency would further ensure that AI serves as an instrument of fairness rather than exclusion.

Accountability and Oversight

AI surveillance introduces complex accountability dilemmas. Decisions made by algorithms can have life-altering consequences, yet it is often unclear who bears responsibility for errors or misuse developers, operators, or policymakers (Mhlambi & Tiribelli, 2022). This “responsibility gap” undermines ethical governance and complicates the enforcement of human rights standards. In many African states, there are limited institutional mechanisms to audit or review AI surveillance systems, allowing misuse to go unchecked.

Moreover, lack of transparency in AI decision-making often referred to as the “black box problem” makes it difficult to challenge wrongful surveillance or arrest. Citizens subjected to algorithmic profiling rarely have access to remedies or appeals. From an ethical perspective, this opacity contradicts democratic principles of accountability and due process. Governments must therefore establish clear regulatory frameworks that define responsibility, ensure transparency, and empower citizens to seek redress for AI-related violations.

Ethical Strategies for Effective AI Surveillance in Counterterrorism

Having analysed the challenges and the ethical implications, it becomes paramount to direct the attention of the developers and those deploying the use of Artificial Intelligence surveillance in counterterrorism to follow the suggested pathways to improve surveillance for effective counterterrorism operations in Nigeria. The following issues should be taken into serious consideration as a means to enhance the rightful use of AI in counterterrorism operations. Attention should be paid to the following elements.

Establishing Robust Legal and Regulatory Frameworks

The first strategy for ensuring ethical AI surveillance is to institutionalize comprehensive legal and regulatory frameworks that define the limits of state surveillance. These frameworks should articulate clear standards for data protection, consent, transparency, and accountability. National legislatures must enact AI governance laws that require human oversight in surveillance operations, restrict data retention, and provide mechanisms for citizen redress in cases of misuse. Importantly, oversight bodies must be independent, adequately funded, and empowered to investigate security agencies without political interference.

Regionally, the African Union and sub-regional bodies such as ECOWAS and the African Commission on Human and Peoples’ Rights should spearhead harmonization efforts. The African Union’s 2022 “Continental Strategy for Artificial Intelligence” provides a foundation for such governance by advocating for ethical standards, data sovereignty, and human

rights protection. Implementing this strategy across member states would help establish uniform principles that promote both national security and human dignity.

Promoting Transparency, Accountability, and Oversight

Transparency and accountability are essential to preventing the misuse of AI in counterterrorism operations. Governments must disclose how AI surveillance systems function, what data they collect, and how decisions are made. Establishing audit trails and publishing periodic reports on AI usage would enhance public trust and demonstrate ethical responsibility. Furthermore, introducing algorithmic transparency allowing independent experts to review and assess the fairness and accuracy of AI models would help detect and mitigate bias or errors.

Accountability also requires clear lines of responsibility among developers, policymakers, and operators. When AI systems cause harm, affected individuals should have access to legal remedies and avenues for appeal. By strengthening public oversight, Africa can ensure that AI surveillance remains a tool for protection rather than coercion. Transparency and accountability thus transform AI from a mechanism of control into an instrument of legitimate governance.

Building Indigenous Capacity and Technological Sovereignty

Developing indigenous capacity is critical to ethical and sustainable AI deployment. African governments should invest in education, research, and innovation ecosystems that nurture expertise in AI ethics, data science, and cybersecurity. Establishing national AI research centres and fostering collaboration between universities, industry, and government agencies can help reduce dependency on foreign technology providers. Capacity-building initiatives should also prioritize ethical training for security personnel to ensure responsible use of AI surveillance tools.

Technological sovereignty enables African states to set their own ethical and operational priorities. By developing homegrown AI solutions, countries can tailor algorithms to local contexts, reduce bias, and protect sensitive data from foreign exploitation. Furthermore, regional cooperation in AI research through platforms like the African Institute for Mathematical Sciences (AIMS) can strengthen continental innovation networks that support secure, ethical, and contextually relevant AI deployment.

Integrating Human Rights and Ethical Governance

Finally, ethical AI surveillance must be grounded in human rights and democratic governance. Security strategies should integrate human rights impact assessments at every stage of AI deployment from design and procurement to implementation and evaluation. Governments must also ensure that counterterrorism operations adhere to principles of necessity, proportionality, and legality. Ethical governance requires collaboration between state institutions, civil society, and academia to monitor the societal impacts of AI.

Embedding human rights into AI governance frameworks strengthens the moral legitimacy of counterterrorism efforts. It also fosters citizen trust, which is indispensable for intelligence sharing and public cooperation. Ethical governance ensures that technological

progress complements rather than compromises democratic stability. Ultimately, integrating ethics into national security strategy represents not just a moral imperative but a strategic necessity for sustainable peace and security in Africa.

Conclusion

Artificial intelligence represents both an opportunity and a challenge for national security in Africa. As terrorism and insurgency evolve in complexity, AI surveillance offers powerful tools for enhancing intelligence gathering, threat detection, and operational precision. Yet, without adequate ethical and legal safeguards, these technologies risk undermining the very freedoms they aim to protect. The African experience demonstrates that technological efficiency alone cannot guarantee security; it must be balanced with moral responsibility and respect for human dignity.

The ethical implications of AI surveillance ranging from privacy violations and algorithmic bias to accountability gaps underscore the need for principled governance. Addressing these challenges requires a multidimensional approach that integrates law, ethics, technology, and human rights. Africa's unique socio-political and cultural contexts must inform this approach, ensuring that AI serves as a force for inclusive security rather than authoritarian control. By embedding ethical considerations into national security policy, African governments can foster a culture of trust, transparency, and legitimacy.

Ultimately, the ethical deployment of AI surveillance in counterterrorism operations will determine whether Africa's technological transformation contributes to peace or perpetuates oppression. The future of national security lies not in unchecked surveillance, but in intelligent systems governed by fairness, accountability, and justice. By aligning AI innovation with democratic values and human rights, Africa can build a secure, ethical, and sovereign technological future.

Recommendations

It is recommended that governments in Africa should:

- a. Adopt comprehensive AI governance laws that clearly define surveillance limits, accountability structures, and human rights safeguards.
- b. Establish independent oversight bodies to monitor AI use in national security, ensuring transparency and preventing abuse.
- c. Invest in local AI research and education to enhance indigenous capacity and reduce reliance on external technology providers.
- d. Integrate human rights assessments into all AI-related counterterrorism initiatives.
- e. Promote regional cooperation under the African Union to develop a harmonized ethical AI framework.
- f. Encourage public awareness and civic engagement to strengthen trust between citizens and security institutions.
- g. Mandate algorithmic transparency to prevent discrimination and bias in AI systems.

-
- h. Ensure that AI procurement contracts include clauses on data protection, ethical compliance, and auditability.

References

- Abebe, R. (2022). Algorithmic justice in global perspective: Lessons from Africa. *Communications of the ACM*, 65(4), 22–26.
- Acharya, A. (2020). The evolution of global security: Norms, ideas, and the African experience. *International Affairs*, 96(6), 1401–1420.
- African Union. (2022). *Continental strategy for artificial intelligence in Africa*. Addis Ababa: African Union Commission.
- Akinola, O. (2023). Artificial intelligence and the ethics of security governance in Africa. *African Security Review*, 32(1), 59–78.
- Amoore, L. (2020). *Cloud ethics: Algorithms and the attributes of ourselves and others*. Duke University Press.
- Baldwin, D. A. (1997). The concept of security. *Review of International Studies*, 23(1), 5–26.
- Crenshaw, M. (2011). *Explaining terrorism: Causes, processes, and consequences*. Routledge.
- Ezeani, E. (2021). Digital intelligence and security governance in Africa. *Journal of African Studies and Development*, 13(4), 89–102.
- Fazlioglu, M. (2021). AI surveillance and data protection in the global south. *Journal of Law, Technology & Policy*, 2021(2), 43–72.
- Feldstein, S. (2019). The global expansion of AI surveillance. *Carnegie Endowment for International Peace*.
- Mhlambi, S. (2020). *African values and the ethics of artificial intelligence*. Montreal AI Ethics Institute.
- Mhlambi, S., & Tiribelli, L. (2022). *Artificial intelligence, ethics, and human rights in Africa*. UNESCO Series on AI and Society.
- UNDP. (2022). *Preventing violent extremism in Africa through data-driven approaches*. United Nations Development Programme.
- UNESCO. (2021). *Recommendation on the ethics of artificial intelligence*. Paris: UNESCO.
- Wright, D., & Kreissl, R. (Eds.). (2014). *Surveillance in Europe*. Routledge