



CLEEN
FOUNDATION
Justice Sector Reform

POLICY BRIEF

Institutionalization of Artificial Intelligence in the Nigeria's Security Architecture:

Safeguarding Rights,
Accountability, and
National Security



PROTECT
RIGHTS



PROMOTE
ACCOUNTABILITY



LEVERAGE AI
RESPONSIBLY



STRENGTHEN
NATIONAL SECURITY

Advancing the responsible and rights-respecting use of
Artificial Intelligence to build a secure, just, and accountable
Nigeria for all.



www.cleen.org



[cleenfoundation](https://www.facebook.com/cleenfoundation)



[@cleenfoundation](https://twitter.com/cleenfoundation)



[@cleenfoundation](https://www.instagram.com/cleenfoundation)



[CLEEN Foundation](https://www.linkedin.com/company/cleen-foundation)



Executive Summary

The rapid evolution of Artificial Intelligence (AI) is reshaping global security governance, redefining how states prevent crime, manage intelligence, secure borders, respond to conflicts, and protect critical national infrastructure. Across the world, governments are increasingly institutionalizing AI-driven systems within their security architectures to improve operational efficiency, predictive capabilities, surveillance coordination, cyber defence, and strategic decision-making. In Nigeria, where insecurity remains multifaceted and dynamic, ranging from terrorism and banditry to cybercrime, kidnapping, violent extremism, and communal conflicts; the integration of AI into security operations is becoming both inevitable and necessary.

Nigeria's security institutions are gradually deploying AI-enabled technologies such as biometric identification systems, digital surveillance platforms, predictive analytics, facial recognition technologies, unmanned systems, and automated data-processing tools to strengthen national security responses. These innovations hold significant promise for improving intelligence gathering, inter-agency coordination, crime detection, emergency response, and public safety outcomes. Properly governed, AI can enhance state capacity, support evidence-based policing, optimize resource deployment, and improve accountability within security operations.

Introduction

The institutionalization of AI within Nigeria's security architecture also introduces profound governance, ethical, legal, and human rights challenges. In the absence of comprehensive regulatory safeguards, AI systems may enable intrusive surveillance, unlawful profiling, algorithmic discrimination, political repression, abuse of citizens' data, and opaque decision-making processes that undermine democratic accountability and public trust. Existing legal and institutional frameworks in Nigeria remain inadequate to address the complexities associated with automated security systems, data governance, algorithmic accountability, transparency obligations, procurement oversight, and independent monitoring of AI deployment.

The growing use of emerging technologies by both state and non-state actors further heightens the urgency for Nigeria to establish a coherent governance framework that balances national security imperatives with constitutional freedoms, human rights protections, and the rule of law. Without deliberate safeguards, AI deployment within the security sector risks deepening civic distrust, exacerbating social inequalities, and weakening democratic institutions. Conversely, failure to modernize security institutions through responsible technological innovation could limit Nigeria's capacity to effectively respond to increasingly sophisticated security threats in a digital age.

Ahead of the Curve:

Why Nigeria's Security Institutions Are Unprepared for AI

Nigeria's public safety and national security challenges are increasingly acquiring a complex digital dimension that analogue institutions are structurally ill-equipped to confront. Violent extremist groups such as Islamic State West Africa Province (ISWAP) are leveraging encrypted digital ecosystems, bot-driven propaganda, and algorithmically amplified radicalization campaigns to recruit, mobilize, and influence vulnerable populations across northern Nigeria and the wider Lake Chad region. At the same time, organized bandit and kidnapping networks are exploiting encrypted communication platforms, geolocation technologies, and digital financial systems to coordinate attacks across multiple state boundaries with increasing sophistication and operational speed.

Beyond conventional security threats, technology-enabled violence is also expanding into civic and social spaces. Gender-based violence has metastasized online through cyberstalking, deepfakes, digitally manipulated intimate imagery, non-consensual content distribution, coordinated harassment campaigns, and other forms of technology-facilitated abuse for which survivors often have little or no accessible legal remedy. The rapid expansion of digital threats has therefore blurred the traditional boundaries between cyber security, public safety, human rights, and national security governance. These are no longer emerging or hypothetical risks; they are present-day realities already reshaping Nigeria's security environment.

Against this backdrop, Nigeria's security institutions remain institutionally and technologically unprepared for the scale and complexity of these evolving threats. The Nigeria Police Force

Core governance challenge: Nigeria's immediate challenge is not merely the absence of technology, but the absence of the democratic, legal, and institutional architecture required to govern it responsibly.

(NPF), alongside other security and law enforcement agencies, continues to face critical deficits in interoperable data systems, digital infrastructure, cyber forensic capabilities, technical expertise, and institutional coordination. Equally concerning is the absence of comprehensive regulatory and accountability frameworks capable of governing the deployment, procurement, oversight, and ethical use of Artificial Intelligence (AI) and emerging surveillance technologies within the security sector.

Where AI-adjacent technologies are already being introduced including facial recognition systems, biometric databases, predictive analytics tools, drone surveillance platforms, and smart city monitoring infrastructure deployment has often occurred in fragmented and opaque ways, with limited legislative scrutiny or public accountability. Several surveillance technologies procured by state institutions and subnational governments operate without clear legal mandates, independent oversight mechanisms, algorithmic bias auditing, transparency obligations, or effective citizen redress systems. This represents the core governance challenge confronting Nigeria today: not merely the absence of technology, but the absence of the democratic, legal, and institutional architecture required to govern it responsibly.

The implications are profound. Ungoverned or poorly regulated AI does not simply fail to produce reform; it can actively undermine democratic accountability, civic freedoms, and institutional legitimacy. Biased predictive systems can reinforce ethnic, religious, gender, or socio-economic profiling. Opaque algorithmic decision-making can shield wrongful arrests, discriminatory targeting, or abusive policing practices from public scrutiny. Surveillance systems deployed without judicial safeguards or

proportionality standards can evolve into instruments of political repression, intimidation, and unlawful monitoring of civic actors, journalists, and opposition voices.

Nigeria's reform experience demonstrates that institutional modernization without accountability safeguards often reproduces old patterns of abuse in technologically advanced forms. Security sector reforms that prioritize operational capacity without strengthening oversight frequently deliver cosmetic transformation while leaving structural governance deficits intact. AI governance must not repeat this trajectory. The integration of Artificial Intelligence into Nigeria's security architecture must therefore be anchored in constitutionalism, rule of law, transparency, human rights protections, and democratic oversight.

If governed responsibly, AI can strengthen intelligence analysis, improve emergency response systems, enhance crime prevention capabilities, support evidence-based policing, and improve service delivery across the security sector. However, without robust safeguards, the same technologies can deepen public distrust, widen inequalities, weaken civic space, and erode the legitimacy of state institutions. The challenge before Nigeria is therefore not whether AI will become embedded within its security ecosystem, but whether the country will develop the institutional maturity, regulatory safeguards, and democratic accountability mechanisms necessary to ensure that technological advancement strengthens rather than undermines national security and citizens' rights.

THREE DOMAINS

One Governance Imperative

CLEEN Foundation identifies three domains where the need is most acute, the potential greatest, and the governance deficit most dangerous.

I. AI in Police and Policing: Governance Before Procurement

The NPF is the primary interface between the Nigerian state and its citizens on matters of security. AI tools for misconduct early warning, multilingual complaint management, evidence cataloguing, and Police Service Commission (PSC) performance monitoring offer genuine potential to advance police accountability. But procurement without governance is the greater risk.

Three conditions are non-negotiable before any AI deployment in policing:

- **Explainability:** Every AI-assisted policing output must be articulable and auditable. Black-box systems that cannot account for their conclusions are inadmissible in any accountability or disciplinary process.
- **Human accountability:** A named officer must be legally responsible for every decision informed by AI. Automation does not dissolve command responsibility.
- **Independent oversight:** Civil society organisations must hold statutory audit rights over NPF AI systems not advisory roles, but legally enforceable ones.

State police reform adds urgency: once formations are operational across thirty-six states and the FCT, AI governance must hold across thirty-seven distinct institutional environments. Federal minimum standards, legislated now, are the only protection against a rights patchwork in which outcomes vary by postcode.

II. An AI-Powered ACJA/L Implementation Tracker: Making Justice Visible

The Administration of Criminal Justice Act (ACJA) 2015 and its state equivalents represent the most significant statutory reform of Nigeria's criminal justice process in a generation. On paper, they protect awaiting-trial persons, mandate bail reviews, and prescribe clear timelines. In practice, compliance is inconsistent, unmonitored, and impunity is the norm. Nigeria's correctional facilities hold more pretrial detainees than convicted persons a crisis hiding in plain sight.

An AI-Powered ACJA/L Implementation Tracker would change the accountability calculus fundamentally. By integrating court registry data, legal aid records, and structured community reporting, the Tracker would:

- Generate automated alerts when remand periods exceed statutory limits, making unlawful detention visible in real time.
- Map systemic bottlenecks by court, prosecutor, and police formation converting scattered non-compliance into legally actionable pattern evidence.
- Produce public-facing compliance dashboards, placing the burden of transparency on institutions rather than on under-resourced civil society monitors.

Critically, the Tracker must be custodied by an independent CSO not a government agency. Its data must fall under NDPA 2023 and remain within Nigerian jurisdiction, with findings validated by an independent review board before informing any enforcement action. Its value lies precisely in independence from the institutions it monitors.

III. AI in Civic Engagement: Empowerment, Not Surveillance

The most consequential misapplication of AI in Nigeria's security context would be to deploy it exclusively as a state tool while leaving citizens without reciprocal capabilities. AI must be a lever of civic power, not only of state power.

Both share a foundational requirement: community consent and governance. AI tools imposed without meaningful participation will be rejected or weaponized. The architecture must be built from the citizen up, not the ministry down.



RECOMMENDATIONS

1. POLICING

The National Assembly should legislate a National AI Policing Governance Standard with binding civil society audit rights as a mandatory condition of any state police license. The PSC should serve as the primary AI regulatory authority for policing.

2. ACJA/L TRACKER

Develop an AI powered Tracking System for compliance with the provisions of the ACJA/L across the country.

3. CIVIC EMPOWERMENT

CLEEN Foundation, drawing on its three decades of community-facing security sector programming, should serve as the lead implementing organization for Nigeria's AI civic empowerment agenda.

4. LEGISLATIVE ANCHOR

Support to Civil Society Organizations like CLEEN Foundation to lead engagement with the National Assembly with the view of providing a legal framework for the adoption of AI in SSR/G



Get in Touch!

www.cleen.org

CLEEN Foundation
27 Moses Majekodunmi Crescent, Utako,
Abuja, Federal Capital Territory, Nigeria

[f](#) [@](#) [X](#) [in](#) @cleenfoundation [✉](mailto:cleen@cleen.org) cleen@cleen.org



SCAN CODE
TO VISIT OUR
WEBSITE