Quest Journals
Journal of Education, Arts, Law and Multidisplinary
Volume 16 ~ Issue 1 (Jan. – Feb. 2026) pp: 129-140
ISSN(Online): 2347-2895
www.questjournals.org

Research Paper

Legal Regulation of Artificial Intelligence-Assisted Human Intelligence Operations in Nigeria: The Legal Safeguards.

KELVIN BRIBENA PhD[1]
Faculty of Law, Niger Delta University,
Wilberforce Island, Bayelsa State, Nigeria

Abstract
This article examined the legal regulation of artificial intelligence-assisted human intelligence operations in Nigeria, with particular focus on AI-supported intelligence gathering and the safeguards required to ensure lawful and accountable deployment. The study adopted a doctrinal and comparative legal research methodology. It examined Nigerian constitutional provisions, regulatory frameworks and policy documents, including the Constitution of the Federal Republic of Nigeria 1999 (as amended), the Nigeria Data Protection Act 2023, the Cybercrimes (Prohibition, Prevention, etc) Act 2015 (as amended in 2024), telecommunications interception regulations and Nigeria's National Artificial Intelligence Strategy. It also draws comparative lessons from international AI governance frameworks, including the European Union Artificial Intelligence Act (2024), UNESCO Recommendation on the Ethics of Artificial Intelligence and OECD AI Principles. The article argued that while existing Nigerian laws provide important foundations for regulating AI-assisted intelligence operations, they do not sufficiently address the unique risks created by AI-driven surveillance, predictive intelligence and automated analytical systems. The found that the absence of dedicated rules governing AI use in intelligence activities create uncertainties regarding human oversight, accountability for algorithmic decisions, transparency obligations and remedies for affected individuals. The article recommended a regulatory approach based on human control, risk assessment, independent oversight, data governance safeguards and clear institutional responsibility. It concluded that Nigeria should embrace AI-enabled intelligence capabilities while ensuring that technological advancement remains subject to constitutional limitations, rule-of-law principles and protection of individual rights.

Keywords: *Artificial Intelligence; Intelligence Operations; National Security; Surveillance; Data Protection; Nigeria; AI Governance; Human Intelligence.*

I. Introduction

Artificial intelligence has become one of the most significant technological developments affecting contemporary national security and intelligence operations. Intelligence agencies across the world increasingly employ AI-supported systems to identify patterns, analyse large datasets, detect security threats, monitor emerging risks and support human decision-making. Unlike traditional intelligence methods, which depend heavily on human collection and interpretation, AI-assisted intelligence operations allow agencies to process information at a scale and speed that would be impossible through human effort alone. The use of AI in intelligence gathering is particularly significant because modern security threats are increasingly digital, decentralised and information-driven. Terrorist networks, cybercriminal groups, organised criminal organisations and foreign influence operations often operate through online platforms and generate vast quantities of digital information.[2] AI systems can assist intelligence officers by identifying relationships between individuals, analysing communication patterns, processing publicly available information and highlighting potential threats requiring further human investigation.

[1] Kelvin Bribena, LLB, BL, LLM, M.Sc, M.Ed, LLD, ACIArb, FNIMN, Head of Department, Jurisprudence and International Law, Faculty of Law, Niger Delta University, Wilberforce Island, Bayelsa State, Nigeria
[2] OECD, *Recommendation of the Council on Artificial Intelligence* (OECD 2019) <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> accessed 18 August 2026; UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (UNESCO 2021) <https://unesdoc.unesco.org/ark:/48223/pf0000381137> accessed 18 August 2026.

For Nigeria, these developments present both opportunities and regulatory challenges. Nigeria faces complex security challenges involving terrorism, cybercrime, financial crimes, organised criminal networks, misinformation campaigns and cross-border threats. AI-supported intelligence capabilities could improve the ability of security institutions to detect and respond to these threats. However, intelligence activities involve some of the most sensitive exercises of state power because they frequently involve surveillance, collection of personal information and restrictions on individual privacy. The legal challenge is therefore not whether Nigeria should permit AI use in intelligence operations. Rather, the central question is how such technology can be deployed while maintaining constitutional safeguards, democratic accountability and respect for fundamental rights. Nigeria currently does not have a standalone Artificial Intelligence Act regulating government intelligence applications. Instead, AI governance operates through a combination of existing data-protection legislation, cybersecurity regulation, constitutional protections and policy initiatives. The Nigeria Data Protection Act (NDPA) 2023 provides the principal statutory framework for personal-data processing, while Nigeria's National Artificial Intelligence Strategy establishes a policy direction for responsible AI development and deployment.[3]

The NDPA is particularly relevant because AI systems depend heavily on personal data. Intelligence-related AI applications may involve processing biometric information, location data, communication records, financial information, online activity and other categories of sensitive personal information. Although the NDPA applies broadly to automated processing of personal data, it was not enacted specifically for intelligence algorithms or national-security AI systems. This creates important legal questions. Can intelligence agencies use AI systems to identify individuals as potential security threats without direct human suspicion? What safeguards should apply when an algorithm produces inaccurate intelligence assessments? Who bears responsibility where an AI-generated recommendation contributes to unlawful surveillance or mistaken targeting? Should individuals affected by AI-assisted intelligence decisions have access to notification, review or remedies?

These questions demonstrate that AI-assisted intelligence operations exist at the intersection of national security and constitutional rights. National security institutions require sufficient flexibility to protect the State, but technological capability cannot remove legal limits on governmental power. Intelligence operations conducted through AI remain exercises of public authority and must therefore operate within legal boundaries.

International developments increasingly recognise this principle. The OECD AI Principles emphasise human-centred AI, transparency and accountability.[4] UNESCO's Recommendation on the Ethics of Artificial Intelligence similarly promotes human oversight, proportionality, fairness and protection of human rights. The European Union Artificial Intelligence Act adopts a risk-based regulatory approach, imposing stronger obligations on high-risk AI applications. While these frameworks were not designed specifically for Nigerian intelligence institutions, they provide useful comparative guidance.[5]

The Nigerian regulatory challenge is therefore developing a framework that recognises the unique sensitivity of intelligence operations while preventing uncontrolled algorithmic surveillance.[6] Excessively restrictive regulation may undermine legitimate national-security objectives, while insufficient regulation may create risks of abuse, discrimination and erosion of privacy rights. This article argues that AI should be treated as an intelligence-supporting tool rather than an autonomous authority. Human intelligence officers and accountable institutions must remain responsible for decisions affecting individuals. Effective regulation should therefore focus on human oversight, lawful data processing, transparency, auditability, proportionality and institutional accountability.

II. Research Objectives

The main objective of this article is to examine the legal regulation of artificial intelligence-assisted human intelligence operations in Nigeria, with particular focus on AI-supported intelligence gathering and legal safeguards. The specific objectives are to:

1. Examine the existing legal framework governing AI and intelligence-supported data processing in Nigeria.
2. Analyse the legal challenges associated with AI-assisted intelligence gathering, particularly regarding privacy, surveillance and accountability.
3. Propose legal safeguards capable of promoting responsible AI use in intelligence operations while protecting fundamental rights.

[3] Nigeria Data Protection Act 2023, ss 24–26.
[4] Constitution of the Federal Republic of Nigeria 1999 (as amended), s 37.
[5] Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), arts 6, 14 and 15.
[6] Nigeria Data Protection Act 2023, s 24.

III. Understanding Artificial Intelligence-Assisted Human Intelligence Operations

Artificial intelligence-assisted human intelligence operations represent a significant evolution in the traditional intelligence cycle. Historically, intelligence operations relied primarily on human collection, human assessment and human decision-making. Intelligence officers gathered information through human sources, surveillance activities, interviews, observation and document analysis before producing assessments for decision-makers. Although technology has always supported intelligence work, the analytical burden remained substantially human.[7]

The emergence of artificial intelligence has altered this model. AI systems can now process enormous volumes of structured and unstructured information, identify relationships within complex datasets, recognise patterns, classify information and generate predictive assessments. In intelligence contexts, AI does not necessarily replace human intelligence officers. Rather, it operates as an analytical capability that enhances human collection and assessment. This distinction is important because the legal risks associated with AI-assisted intelligence operations arise not merely from the existence of AI systems but from the extent to which those systems influence state decisions. An AI tool that assists an intelligence analyst in organising publicly available information presents different legal concerns from an AI system that independently identifies individuals as security threats, recommends surveillance measures or influences operational decisions. AI-supported intelligence gathering may involve several technological applications.

First, machine learning-based intelligence analysis enables systems to examine large datasets and identify patterns that may not be immediately visible to human analysts. For example, an intelligence agency investigating organised criminal networks may use AI to analyse connections between financial transactions, communication records, online activities and geographical movements.

Secondly, natural language processing (NLP) allows AI systems to analyse large quantities of text-based information, including social media content, intercepted communications where lawfully obtained, online publications and intelligence reports. NLP systems may assist analysts by identifying themes, translating materials or detecting potential indicators of coordinated activity.

Thirdly, facial recognition and biometric analysis technologies allow authorities to compare images, identify individuals and analyse biometric information. While these technologies may support legitimate security objectives, they create significant legal concerns because biometric data is among the most sensitive categories of personal information. The misuse of biometric intelligence systems can produce extensive surveillance capabilities affecting individuals who are not suspected of criminal conduct.

Fourthly, open-source intelligence (OSINT) enhanced by AI allows agencies to analyse publicly available information from websites, social media platforms, news sources and other digital environments. AI can improve the speed at which analysts process publicly available information, but the distinction between publicly accessible information and legally unrestricted information processing remains important. The fact that information is publicly available does not automatically remove privacy concerns.

Fifthly, predictive intelligence systems attempt to identify potential risks before events occur. These systems may analyse historical data to identify patterns associated with criminal activity, security threats or social instability. However, predictive intelligence creates significant legal concerns because algorithmic predictions may reproduce historical biases and create situations where individuals are subjected to heightened scrutiny because of statistical associations rather than evidence of individual wrongdoing.

The movement from traditional intelligence analysis to AI-supported intelligence therefore creates a fundamental legal question: what role should AI be permitted to play in exercises of state power? A useful distinction here that grants answer to the above question is between three levels of AI involvement:

(a) AI as an Analytical Assistance Tool: At the lowest level of intervention, AI performs administrative or analytical functions while human officials retain full control. Examples include sorting information, identifying duplicate records, translating materials or assisting analysts in reviewing large datasets. This form of AI use generally presents lower legal risks because human officials remain responsible for interpreting information and making decisions.

(b) AI as an Intelligence Recommendation System: At the second level, AI produces assessments or recommendations that may influence operational decisions. Examples include identifying suspicious patterns, ranking potential threats or suggesting investigative priorities. This category creates greater legal concerns because decision-makers may rely excessively on algorithmic outputs. The problem is particularly acute where officials assume that AI-generated assessments are objective merely because they are produced by technology.

(c) AI as an Automated Decision-Making System: At the highest level, AI systems may effectively determine outcomes with limited human intervention. Examples could include automatically placing individuals on watchlists, initiating surveillance measures or determining threat classifications. This raises the most serious legal

[7] Stephen Mason, Electronic Evidence (6th ed., Institute of Advanced Legal Studies, University of London, 2021) 10 - 11

concerns because automated decisions affecting fundamental rights require strong safeguards. A person should not lose liberty, privacy or reputation because of an opaque algorithmic assessment that cannot be meaningfully challenged. The central regulatory principle should therefore be that AI enhances intelligence capability but does not transfer legal responsibility from humans to machines.

3.1 Artificial Intelligence and the Changing Nature of Human Intelligence (HUMINT)

Human intelligence remains central to national security because intelligence is ultimately concerned with understanding human behaviour, intentions and motivations. AI can identify patterns, but it does not possess human judgment, contextual understanding or moral reasoning. Intelligence decisions often require consideration of political, social, cultural and historical factors that cannot be reduced entirely to computational analysis. This is particularly relevant in Nigeria, where security challenges are shaped by complex social realities.[8] Issues involving terrorism, communal violence, kidnapping, cybercrime, economic crime and political instability often require contextual understanding beyond statistical prediction.

Consequently, AI should be viewed as an enhancement to HUMINT rather than a replacement. Intelligence officers remain necessary to verify information, evaluate reliability, consider alternative explanations and make legally accountable decisions. The continued importance of human involvement is recognised internationally. The OECD AI Principles emphasise that AI systems should be designed to respect human autonomy and allow appropriate human oversight,[9] while UNESCO's AI ethics framework identifies human responsibility and oversight as essential requirements for trustworthy AI governance.

For Nigerian intelligence operations, this principle has significant implications. The existence of AI-generated intelligence should not automatically justify surveillance, investigation or adverse action. Human officers must critically evaluate AI outputs and consider whether information is reliable, relevant and proportionate.

3.2 Intelligence Data and the Problem of Scale

The greatest advantage of AI-assisted intelligence is also one of its greatest legal risks: scale. Traditional intelligence operations were limited by human capacity. Officers could review only a limited number of documents, communications or observations. AI systems remove this limitation by enabling automated processing of enormous datasets. However, increased analytical capacity creates the possibility of excessive surveillance. A system capable of analysing millions of individuals' online activities may produce useful security information, but it may also process information relating to individuals who have no connection to any security threat. This raises questions about proportionality.

A core principle of modern data-protection law is that personal information should be processed only for specified, legitimate purposes and only to the extent necessary to achieve those purposes. The Nigeria Data Protection Act 2023 reflects these principles through obligations relating to lawful processing, purpose limitation, data minimisation and accountability.

The difficulty is that intelligence activities traditionally operate within secrecy. Intelligence agencies may legitimately require confidentiality regarding sources, methods and investigations. However, secrecy cannot eliminate the need for legal safeguards. A democratic state must maintain mechanisms ensuring that confidential intelligence activities remain subject to lawful authority.

3.3 AI-Assisted Surveillance and National Security

Surveillance is among the most sensitive applications of AI in intelligence operations. AI can enhance surveillance through facial recognition, location analysis, behavioural pattern identification and automated monitoring of digital environments. From a national-security perspective, these capabilities offer significant benefits. They may assist authorities in identifying terrorist networks, preventing attacks, investigating organised crime and protecting critical infrastructure. However, surveillance technologies also create risks of disproportionate interference with individual rights. The concern is not simply whether surveillance occurs, but whether surveillance is: legally authorised; necessary for a legitimate objective; proportionate to the threat; subject to oversight; and capable of review.

Section 37 of the Constitution of the Federal Republic of Nigeria 1999 protects the privacy of citizens, including privacy of homes, correspondence, telephone conversations and telegraphic communications.[10]

[8] Stephen Mason, Electronic Evidence (6th ed., Institute of Advanced Legal Studies, University of London, 2021) 20-21

[9] Organisation for Economic Co-operation and Development (OECD), Digital Economy Outlook <https://www.oecd.org> accessed 24 August 2026

[10] Constitution of the Federal Republic of Nigeria 1999 (as amended), section 37.

Although constitutional privacy rights are not absolute, any interference by public authorities must operate within legal limits.

The challenge for Nigeria is that existing privacy protections were developed before modern AI surveillance capabilities became widespread. Traditional interception rules generally assume targeted surveillance of identifiable persons. AI enables broader forms of monitoring where systems search large datasets to identify possible threats. This creates a regulatory gap between traditional surveillance law and contemporary AI capabilities.

3.4 The Importance of Human-in-the-Loop Governance

A central safeguard for AI-assisted intelligence operations is the requirement for meaningful human oversight. Human oversight should not mean merely that an officer clicks an approval button after an AI system produces a recommendation. Effective oversight requires that the human decision-maker: understands the purpose and limitations of the AI system; has authority to reject the AI recommendation; receives sufficient information to evaluate reliability; considers alternative explanations; and remains legally responsible for the final decision.

The European Union Artificial Intelligence Act reflects this approach by requiring appropriate human oversight for high-risk AI systems. Although Nigeria is not bound by the EU framework, the principle is relevant because intelligence operations involve decisions capable of affecting fundamental rights. For Nigerian intelligence agencies, human oversight should become a statutory requirement rather than merely an internal administrative practice.

IV. Existing Nigerian Legal Framework Governing AI-Assisted Intelligence Operations

Nigeria's regulation of AI-assisted intelligence operations currently operates through multiple overlapping legal frameworks rather than a single dedicated AI intelligence statute. These frameworks provide important safeguards but were generally developed before the emergence of advanced AI systems. The relevant legal sources include:

1. The Constitution of the Federal Republic of Nigeria 1999 (as amended);
2. The Nigeria Data Protection Act 2023;[11]
3. The Cybercrimes (Prohibition, Prevention, etc) Act 2015;[12]
4. Telecommunications interception regulations;[13]
5. National cybersecurity policies; and
6. Nigeria's National Artificial Intelligence Strategy.

4.1 Constitutional Privacy Protection

The constitutional foundation for regulating AI-supported intelligence operations is section 37 of the 1999 Constitution, which provides that: "The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected." Although drafted before the emergence of artificial intelligence, this provision remains relevant because AI intelligence systems frequently involve the collection and analysis of personal information. The constitutional protection raises important questions regarding the use of: facial recognition databases; automated communication analysis; location tracking; social-media monitoring; biometric intelligence systems; and predictive threat assessments. The Constitution does not expressly prohibit surveillance. However, it establishes a legal principle that privacy is a protected interest requiring justification where state authorities interfere with personal information.

4.2 Nigeria Data Protection Act 2023 and AI Intelligence Processing

The Nigeria Data Protection Act 2023 (NDPA) represents the most significant development in Nigeria's data-governance framework and provides the primary legal foundation for regulating AI systems that process personal information. Although the Act does not expressly regulate artificial intelligence-assisted intelligence operations, many of its principles directly apply to government use of AI where such systems involve the collection, analysis, storage or disclosure of personal data.

This is particularly important because AI systems are fundamentally dependent on data. An AI intelligence system cannot identify patterns, classify individuals or generate predictive assessments without access to significant quantities of information. In intelligence environments, this information may include biometric identifiers, communication records, location information, financial records, online activities and information obtained from public or private sources.

---

[11] Nigeria Data Protection Act 2023, s 28; Nigeria Data Protection Commission, *General Application and Implementation Directive 2025* <https://ndpc.gov.ng> accessed 18 August 2026.

[12] Cybercrimes (Prohibition, Prevention, etc) Act 2015 (Nigeria), ss 38–40.

[13] Nigerian Communications Act 2003; Nigerian Communications Commission, *Lawful Interception of Communications Regulations* < https://www.ncc.gov.ng> accessed 18 August 2026.

The NDPA adopts several principles that are relevant to AI-assisted intelligence operations. Section 24 establishes obligations relating to lawful processing, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, security and accountability.[14] These principles provide a framework for evaluating whether an AI intelligence system is being deployed in a manner consistent with lawful data processing.

4.2.1 Lawful Basis for AI Intelligence Processing

A fundamental requirement under data-protection law is that personal data processing must have a lawful basis. Section 25 of the NDPA provides that processing must be based on one or more recognised lawful grounds, including consent, contractual necessity, legal obligation, vital interests, public interest or legitimate interests, subject to applicable limitations.[15]

Intelligence operations present a unique challenge because they often cannot depend on consent. A person under intelligence observation will generally not be aware that their information is being processed, and requiring consent would undermine legitimate security operations. Consequently, government intelligence processing would typically depend on legal obligation or public-interest grounds. However, reliance on national security objectives cannot create unlimited authority to collect and analyse personal data. The existence of a security purpose does not eliminate the requirement that processing be necessary, proportionate and authorised by law.

This distinction is important because AI systems create a risk of function creep. Data collected for one legitimate purpose may later be used for unrelated intelligence analysis. For example, information collected during a cybersecurity investigation could potentially be repurposed for broader behavioural profiling unless appropriate restrictions exist.

The principle of purpose limitation therefore becomes particularly important. Intelligence agencies using AI should clearly define: the purpose for which data is collected; the categories of persons whose information may be processed; the period for which information may be retained; the officials authorised to access the information; and the circumstances permitting further use. Without such limitations, AI may transform targeted intelligence collection into broad population monitoring.

4.2.2 Automated Decision-Making and Human Review

One of the most relevant provisions for AI governance is the NDPA's approach to automated decision-making. Modern AI systems may produce decisions or recommendations affecting individuals without direct human involvement. Examples include: automatically assigning risk scores; identifying persons as potential security threats; ranking individuals for further investigation; determining suspicious activity patterns.

The legal concern is that algorithmic outputs may appear objective while concealing errors, bias or incomplete assumptions. The NDPA recognises protections relating to decisions based solely on automated processing where such decisions produce legal or similarly significant effects.[16] Although intelligence operations may involve national-security considerations, the underlying principle remains important: individuals should not be subjected to significant consequences solely because an algorithm produced a conclusion.

For intelligence agencies, this requires a human-review model. AI-generated intelligence should be treated as an analytical input rather than a final determination. For example, if an AI system identifies an individual as potentially linked to a terrorist organisation, the system's output should trigger further human investigation rather than automatically justify surveillance, arrest or restriction of rights.

4.2.3 Sensitive Personal Data and Biometric Intelligence

AI-supported intelligence operations frequently rely on sensitive personal data. The NDPA provides enhanced protection for certain categories of information, including biometric data and other forms of sensitive personal information.[17]

Biometric intelligence raises particularly serious concerns because unlike passwords or identification numbers, biometric characteristics cannot easily be changed. A compromised password can be replaced; compromised biometric information may permanently affect an individual. AI-powered facial recognition systems demonstrate this challenge. A facial-recognition database capable of identifying individuals in public spaces may provide significant security benefits. However, if deployed without appropriate safeguards, it may enable continuous monitoring of citizens who have committed no offence. The legal question is therefore not whether biometric intelligence should ever be used. In legitimate circumstances, such technology may serve important

[14] Nigeria Data Protection Act 2023, ss 24–26.
[15] Nigeria Data Protection Act 2023, s 25.
[16] Nigeria Data Protection Act 2023, s 37.
[17] OECD, *Recommendation of the Council on Artificial Intelligence* (OECD 2019) <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> accessed 18 August 2026.

security purposes. The question is whether its deployment satisfies: necessity; proportionality; accuracy requirements; access restrictions; retention limits; and independent oversight.

4.2.4 Data Protection Impact Assessments and AI Systems

The NDPA introduces obligations concerning privacy impact assessments for processing activities likely to create significant risks to individuals. This requirement has particular relevance for AI intelligence systems. Before deploying an AI surveillance or analytical platform, intelligence agencies should assess: what categories of data the system processes; whether the processing is necessary; possible discriminatory outcomes; cybersecurity risks; risks of misuse; human oversight mechanisms; retention practices. A privacy impact assessment should not be treated as a bureaucratic document. It should operate as a governance mechanism allowing institutions to identify risks before deploying technology capable of affecting fundamental rights.

4.3 Cybercrimes Act 2015 (as amended in 2024) and Digital Intelligence Gathering

The Cybercrimes (Prohibition, Prevention, etc) Act 2015 provides another important component of Nigeria's legal framework for digital intelligence operations. The Act was enacted primarily to address cybercrime, cybersecurity threats and related offences. However, several of its provisions are relevant to intelligence gathering because cyber investigations often require access to digital information. The Act recognises the importance of cooperation between law-enforcement institutions, service providers and relevant authorities in investigating cyber offences. The increasing use of AI in cyber investigations creates new possibilities. AI systems may assist investigators by: identifying malware patterns; analysing cyberattack indicators; correlating information from multiple sources; detecting suspicious digital activity; assisting forensic examination. However, the Act was enacted before the widespread adoption of generative AI and advanced machine-learning systems. It therefore does not directly address issues such as: algorithmic profiling; automated cyber-risk scoring; AI-generated intelligence reports; autonomous investigative recommendations. This creates a regulatory gap.

The Cybercrimes Act provides legal authority for certain investigative activities, but it does not answer the broader governance question of how AI systems used during those investigations should be controlled.[18] For example, if an AI system analyses millions of online accounts and produces a list of potential cybercrime suspects, the legal framework must determine: what evidence supports inclusion on the list; who verifies the algorithmic assessment; how errors are corrected; how long information is retained; and whether affected individuals have any legal remedy.

4.4 Telecommunications Interception and AI-Enhanced Surveillance

Telecommunications surveillance represents one of the most sensitive areas where AI may expand state intelligence capabilities. Nigeria's telecommunications framework permits lawful interception under regulated conditions. The Nigerian Communications Act 2003 provides the legal basis for regulating telecommunications activities, while the Nigerian Communications Commission has issued guidelines relating to lawful interception and communication monitoring.[19]

Traditional interception involves obtaining access to specific communications through authorised procedures. AI changes the nature of surveillance by enabling analysis across larger datasets. An AI-enhanced surveillance system may not simply intercept one communication. Instead, it may: analyse communication patterns; identify relationships between users; detect behavioural changes; predict possible future activities.

This creates a shift from targeted surveillance to predictive surveillance. Targeted surveillance asks: Is there sufficient evidence to monitor this specific person?

Predictive surveillance asks: Which individuals or groups appear statistically likely to represent a future risk?

The second approach creates more significant constitutional concerns because individuals may become subjects of intelligence attention based on probability rather than conduct. A democratic legal system must therefore ensure that AI does not reduce constitutional protections through technological capability.

V. Legal Challenges of AI-Assisted Intelligence Gathering in Nigeria

5.1 Privacy Versus National Security

The central legal tension surrounding AI-assisted intelligence operations is the relationship between privacy and national security. National security is a legitimate governmental objective. The State has a duty to

[18] *Roman Zakharov v Russia* App no 47143/06 (European Court of Human Rights, 4 December 2015); *Big Brother Watch and Others v United Kingdom* App nos 58170/13, 62322/14 and 24960/15 (European Court of Human Rights, 25 May 2021).

[19] OECD, *Recommendation of the Council on Artificial Intelligence* (OECD 2019) <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> accessed 18 August 2026.

protect citizens against terrorism, cybercrime, organised crime and other threats. Intelligence institutions require effective tools to perform this function. However, national security cannot operate as an unlimited exception to legal rights. The difficulty created by AI is that it allows intelligence agencies to collect and analyse information on a scale previously impossible. A traditional surveillance operation may focus on a defined suspect. An AI system may process information concerning thousands or millions of individuals in order to identify patterns. This creates a proportionality problem.

The legal question should therefore not simply be: Does the government have a security purpose?

Rather: Is the method of AI-enabled information processing necessary and proportionate to achieving that purpose?

The European Court of Human Rights has repeatedly recognised that surveillance regimes require adequate safeguards against abuse, including clear rules concerning authorisation, duration, storage, access and oversight. Although Nigeria is not bound by European human-rights jurisprudence, these principles provide persuasive comparative guidance because they address universal concerns regarding state surveillance.

5.2 Algorithmic Bias and Discriminatory Intelligence Outcomes

AI systems learn from existing data. Where historical data contains social, institutional or investigative biases, AI systems may reproduce those patterns.[20] This is particularly concerning in intelligence operations because algorithmic errors may have serious consequences. For example, an AI system trained on historical crime data may identify certain locations, communities or demographic groups as higher-risk because previous enforcement practices focused disproportionately on those areas. The AI system may then reinforce the same pattern by directing additional surveillance toward those communities. The problem is not that AI intentionally discriminates. The problem is that mathematical accuracy does not automatically equal legal fairness. An intelligence algorithm can produce technically correct predictions while still generating legally unacceptable outcomes. Therefore, AI intelligence systems require: representative training data; bias testing; independent evaluation; continuous monitoring; human review.

5.3 Lack of Transparency and Explainability

One of the major challenges associated with AI systems is their opacity. Many advanced AI models operate through complex processes that are difficult even for developers to explain fully. This creates the "black box" problem. In intelligence contexts, opacity creates additional concerns because secrecy is already inherent in intelligence activities. If both the intelligence operation and the algorithmic process are hidden, accountability becomes extremely difficult. A person affected by an AI-assisted intelligence decision may have no knowledge: that AI was used; what information influenced the assessment; whether the system made an error; who approved the decision.

The principle of explainability does not necessarily require intelligence agencies to disclose operational secrets. However, internal accountability mechanisms should exist to ensure that authorised officials can understand and review AI outputs.

5.4 Accountability Gaps and Responsibility for AI-Assisted Intelligence Decisions

A fundamental legal challenge created by artificial intelligence-assisted intelligence operations is determining responsibility when AI-generated information contributes to an unlawful or harmful outcome. Traditional intelligence structures are based on identifiable human actors. An intelligence officer collects information, an analyst evaluates it, a supervisor approves operational action and institutional authorities remain responsible for decisions taken by the agency. AI introduces additional complexity because decisions may be influenced by systems developed by external vendors, trained on datasets created by unknown sources and operated through processes that may not be easily explainable. This creates uncertainty regarding where legal responsibility should attach. For example, if an AI system incorrectly identifies an individual as a security threat and that assessment results in unlawful surveillance, detention or reputational harm, several actors may potentially be involved: the intelligence officer who relied on the AI output; the supervisor who approved operational action; the intelligence agency deploying the system; the government authority responsible for procurement; the technology provider that developed the AI model. A regulatory framework that allows responsibility to become fragmented among these actors creates an accountability gap.

The principle that technology should not become an excuse for avoiding responsibility is increasingly recognised in AI governance. The OECD AI Principles emphasise accountability as a core requirement, providing that AI actors should be responsible for the proper functioning of AI systems and respect applicable laws

[20] Regulation (EU) 2024/1689 (Artificial Intelligence Act).

throughout their lifecycle.[21] For intelligence operations, this principle requires that the state agency deploying AI remains primarily responsible for decisions made through AI-supported systems. A government institution cannot transfer responsibility to a private technology provider merely because the algorithm was externally developed. This approach is consistent with existing public-law principles. Public authorities remain accountable for exercises of state power even where they rely upon contractors, consultants or technological systems. The use of AI should therefore not create a legal situation where no institution accepts responsibility.

5.5 Evidential Reliability of AI-Generated Intelligence

Another emerging challenge concerns the evidential status of information generated or analysed through AI systems. Intelligence information and admissible evidence are not identical concepts. Intelligence agencies frequently operate on incomplete information, indicators and assessments designed to guide decision-making. Courts, however, require evidence that satisfies legal standards concerning relevance, reliability and admissibility. AI may assist intelligence collection, but its outputs cannot automatically be treated as proof of wrongdoing. This distinction is particularly important where AI systems generate: threat assessments; behavioural predictions; facial-recognition matches; automated classifications; risk scores.

An AI-generated conclusion may indicate that further investigation is required, but it should not replace legally admissible evidence. For example, a facial-recognition system may identify an individual as matching an image obtained during an investigation. However, the reliability of that identification depends on several factors: quality of the original image; accuracy rate of the system; training data; possibility of false matches; human verification procedures. The legal system must therefore avoid what may be described as automation bias the tendency of human decision-makers to assume that technological outputs are inherently more reliable than human judgment.

Nigerian evidence law has traditionally focused on human testimony, documentary evidence and expert evidence. The Evidence Act 2011 recognises electronic evidence, particularly through section 84, which establishes requirements for admissibility of statements contained in electronic devices.[2] However, AI-generated intelligence presents a more complex question. The issue is not merely whether the information exists electronically, but whether the method through which the information was generated can be sufficiently explained and challenged. Future Nigerian regulation should therefore establish standards concerning: authentication of AI-generated material; disclosure of relevant algorithmic information where appropriate; expert examination; preservation of original data; human verification before operational use.

5.6 The Absence of Dedicated AI Intelligence Regulation

Perhaps the most significant regulatory weakness in Nigeria is the absence of legislation specifically addressing AI use in intelligence and national-security operations. Existing laws provide important protections, but they were not drafted with contemporary AI capabilities in mind. The Nigeria Data Protection Act regulates personal-data processing. The Cybercrimes Act regulates cyber offences. Telecommunications regulations address interception. Constitutional provisions protect privacy. However, none of these instruments comprehensively addresses questions such as: whether intelligence agencies may deploy facial-recognition systems; whether predictive policing algorithms may be used; what level of human review is required; how AI models should be audited; what transparency obligations apply; how individuals may challenge AI-related decisions.

This regulatory gap creates uncertainty for both government institutions and citizens. From an institutional perspective, intelligence agencies require clarity regarding permissible AI deployment. From a rights perspective, citizens require assurance that AI does not create unrestricted surveillance powers.

A dedicated regulatory framework does not necessarily require a separate "Artificial Intelligence Act". Instead, Nigeria could adopt sector-specific AI governance rules addressing high-risk government uses, including intelligence, law enforcement and national security.

VI. Comparative Lessons from International AI Governance Models

Although Nigeria must develop a framework suited to its constitutional and security environment, international AI governance developments provide useful comparative lessons.

6.1 European Union Artificial Intelligence Act (2024)

The European Union Artificial Intelligence Act represents the first comprehensive AI regulatory framework adopted by a major jurisdictional bloc. It adopts a risk-based approach, categorising AI systems according to their

[21] UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (UNESCO 2021) <https://unesdoc.unesco.org/ark:/48223/pf0000381137> accessed 18 August 2026.

potential impact on individuals and society.[22] High-risk AI systems are subject to enhanced obligations, including: risk-management systems; data governance requirements; technical documentation; record keeping; transparency obligations; human oversight.

The EU framework is particularly relevant to intelligence operations because it recognises that not all AI applications create identical risks. A simple administrative AI tool should not be regulated in the same way as a system capable of affecting fundamental rights. However, national-security applications create complexity because many states traditionally treat intelligence activities as sensitive areas requiring confidentiality. The EU model demonstrates that security considerations do not necessarily eliminate the need for safeguards. The lesson for Nigeria is not to copy the EU framework entirely but to adopt its central principle: the greater the potential impact of an AI system on individual rights, the stronger the governance requirements should be.

6.2 UNESCO Recommendation on the Ethics of Artificial Intelligence

UNESCO's Recommendation on the Ethics of Artificial Intelligence provides a global normative framework based on human rights, transparency, fairness and accountability.[23] The Recommendation identifies several principles relevant to intelligence operations:

Human oversight: AI systems should remain subject to human control, particularly where decisions affect human rights.

Proportionality: AI deployment should be necessary and appropriate for the intended purpose.

Transparency: Individuals and institutions should understand how AI systems operate to the extent necessary for accountability.

Accountability: Institutions deploying AI should remain responsible for its impacts.

These principles are particularly relevant for Nigeria because they provide a governance model that does not require abandoning national-security objectives.

6.3 OECD AI Principles

The OECD AI Principles, adopted in 2019 and updated subsequently, provide another influential framework for responsible AI governance.[24] The Principles emphasise: inclusive growth; human-centred values; transparency; robustness and security; accountability.

For intelligence agencies, the principles of robustness and accountability are particularly important. An intelligence AI system must be reliable, secure against manipulation and subject to responsible institutional oversight.

AI systems used in security contexts may become targets for adversarial manipulation. A malicious actor who compromises an intelligence algorithm could distort threat assessments, create false intelligence or manipulate operational priorities. Therefore, cybersecurity must be considered part of AI governance.

VII. Proposed Legal Safeguards for AI-Assisted Intelligence Operations in Nigeria

A balanced Nigerian framework should neither prohibit AI use in intelligence operations nor permit unrestricted deployment. Instead, regulation should establish safeguards ensuring that AI remains consistent with constitutional principles.

7.1 Establish a Human Oversight Requirement: The first safeguard should be a legal requirement that AI systems used in intelligence operations remain subject to meaningful human oversight. This should include: mandatory human review before significant decisions; identification of responsible officers; authority to reject AI recommendations; documentation of human reasoning. The law should prohibit purely automated decisions that result in significant restrictions on individual rights.

7.2 Introduce AI Impact Assessments for Intelligence Systems: Before deploying high-risk AI systems, intelligence agencies should conduct AI impact assessments. Such assessments should examine: purpose of deployment; categories of data processed; potential privacy effects; accuracy limitations; discrimination risks; security vulnerabilities; oversight mechanisms. The assessment should be reviewed by an appropriate oversight body.

7.3 Create Independent Oversight Mechanisms: Intelligence operations require confidentiality, but secrecy cannot eliminate accountability. Nigeria should strengthen oversight mechanisms capable of reviewing AI deployment by intelligence institutions. Possible oversight functions include: reviewing AI procurement; auditing algorithmic systems; examining complaints; monitoring compliance; investigating misuse. Oversight does not require public disclosure of sensitive intelligence methods. It requires lawful accountability within appropriate institutions.

---

[22] OECD, *Artificial Intelligence in Society* (OECD Publishing 2019) doi:10.1787/eedfee77-en.

[23] UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (UNESCO 2021) <https://unesdoc.unesco.org/ark:/48223/pf0000381137> accessed 18 August 2026.

[24] OECD, *Artificial Intelligence in Society* (OECD Publishing 2019) <doi:10.1787/eedfee77-en.>

7.4 Establish AI Audit and Record-Keeping Requirements: Intelligence agencies deploying AI should maintain records showing: what AI systems are used; their purpose; data sources; responsible officials; operational limitations; review procedures. Audit trails are essential because accountability requires the ability to reconstruct how a decision was reached. Without records, it becomes impossible to determine whether an error resulted from human misconduct, technical failure or inappropriate reliance on AI.

7.5 Develop Clear Rules on Data Retention and Deletion: AI systems encourage large-scale data accumulation. However, retaining information indefinitely creates significant privacy risks. Regulation should establish: retention periods; deletion procedures; access controls; review requirements. Information that no longer serves a lawful intelligence purpose should not remain permanently within government databases.

7.6 Regulate Private AI Vendors Supporting Intelligence Agencies: Many governments increasingly rely on private technology companies for AI capabilities. This creates a need for clear contractual and legal obligations. Private vendors supporting Nigerian intelligence institutions should be subject to requirements concerning: data security; confidentiality; system testing; accuracy standards; audit cooperation; prohibition of unauthorised secondary use. The state must remain responsible for decisions even where private companies provide technological tools.

7.7 Develop AI-Specific Training for Intelligence Personnel: Legal regulation alone cannot guarantee responsible AI use. Intelligence officers must understand: AI limitations; algorithmic bias; data-protection obligations; cybersecurity risks; evidential requirements. Human oversight is meaningful only when decision-makers understand the systems they are supervising.

VIII. Conclusion

Artificial intelligence-assisted human intelligence operations represent one of the most significant transformations in modern security governance. For Nigeria, AI presents substantial opportunities to strengthen intelligence capabilities, improve threat detection, enhance cybersecurity investigations and support evidence-based decision-making.[25] In a security environment characterised by terrorism, cybercrime, organised criminal networks and increasingly complex digital threats, artificial intelligence can provide valuable analytical capabilities that traditional intelligence methods alone may not achieve. However, the adoption of AI in intelligence operations also introduces significant legal challenges. Unlike traditional intelligence tools, AI systems can analyse information at unprecedented scale, generate predictive assessments and influence decisions concerning individuals who may never have been directly investigated. These capabilities create risks relating to privacy, surveillance, accountability, discrimination and the concentration of state power.

The central legal issue is therefore not whether Nigeria should use artificial intelligence in intelligence operations. The more important question is how such use should be regulated to ensure that technological capability remains subject to legal control. This article has demonstrated that Nigeria possesses several legal instruments relevant to AI-supported intelligence gathering. The Constitution protects privacy rights under section 37; the Nigeria Data Protection Act 2023 establishes principles governing personal-data processing; the Cybercrimes Act 2015 provides a framework for digital investigations; telecommunications regulations regulate lawful interception; and the National Artificial Intelligence Strategy provides a policy foundation for responsible AI development. Nevertheless, these frameworks remain insufficient to address the specific risks created by AI-assisted intelligence operations. Existing laws regulate data processing and surveillance generally but do not adequately address issues such as algorithmic accountability, AI transparency, predictive intelligence, automated decision-making, algorithmic bias and institutional responsibility.

A major concern is that AI may create an accountability gap. If intelligence decisions become influenced by complex algorithms, responsibility must not disappear between the technology provider, government institution and individual officer. The deployment of AI cannot transfer legal responsibility from human decision-makers to machines. Intelligence agencies must remain accountable for the systems they use and the decisions made through those systems. The article therefore proposes a human-centred regulatory approach. AI should operate as an intelligence-supporting tool rather than an autonomous decision-maker. Human officers must retain meaningful authority to evaluate, reject or modify AI-generated assessments. Decisions affecting fundamental rights should never depend solely on algorithmic outputs.

Nigeria should also develop AI-specific governance mechanisms for high-risk government applications. These should include mandatory AI impact assessments, algorithmic auditing, record-keeping requirements, data-retention limitations, independent oversight and clear rules governing private technology providers supporting intelligence operations.

---

[25] National Centre for Artificial Intelligence and Robotics (NCAIR), *Nigeria National Artificial Intelligence Strategy* (Federal Ministry of Communications, Innovation and Digital Economy 2024) <https://ncair.nitda.gov.ng/wp-content/uploads/2024/08/National-AI-Strategy_01082024-copy.pdf> accessed 18 August 2026.

At the same time, regulation must recognise the legitimate needs of national-security institutions. Excessive restrictions may prevent agencies from using technology necessary to protect citizens. The objective should therefore not be technological limitation but responsible deployment.

The experience of international AI governance frameworks demonstrates that effective regulation is possible without preventing innovation. The OECD AI Principles, UNESCO Recommendation on the Ethics of Artificial Intelligence and European Union Artificial Intelligence Act all recognise that AI development must be balanced with human rights, accountability and transparency. Nigeria can draw from these approaches while developing a framework consistent with its constitutional structure and security realities.

Ultimately, AI-assisted intelligence operations should be governed by a simple principle: technology may enhance intelligence capability, but it must not replace legal responsibility. The legitimacy of Nigeria's future intelligence architecture will depend not only on its ability to identify threats but also on its ability to demonstrate that security objectives are pursued within the boundaries of law, constitutional rights and democratic accountability.