



AI-DRIVEN PREDICTIVE POLICING AND EMERGING SECURITY CHALLENGES IN NIGERIA

LAWAL ODUNAYO FUNKE

Department of Computer Science, Oyo State College of Education, Lanlate, Oyo State.

adeayo200746@gmail.com

ABSTRACT

Nigeria continues to experience severe insecurity, including insurgency, banditry, kidnapping, and urban violence, which have overwhelmed traditional policing approaches. In response, there is growing interest in the use of Artificial Intelligence (AI)-driven predictive policing as a technological tool to enhance crime prevention and security management. However, its applicability, effectiveness, and governance implications in the Nigerian context remain underexplored. This study examines the role of AI-driven predictive policing in addressing insecurity in Nigeria. It adopts a qualitative research design based on a systematic review of academic literature, policy documents, and comparative analysis of predictive policing practices in selected countries, including the United States, the United Kingdom, China, and African states such as Kenya, Rwanda, and South Africa. The findings reveal that predictive policing can enhance security operations by improving crime mapping, early warning systems, and resource allocation. However, its implementation also raises significant concerns, including algorithmic bias, weak regulatory frameworks, privacy violations, and limited public trust in law enforcement institutions. The study further shows that Nigeria's current legal and institutional structures, including the Nigerian Data Protection Act and constitutional privacy provisions, are not adequately prepared for the large-scale deployment of AI-based policing systems. It concludes that predictive policing should be adopted as a supportive tool within a strongly regulated framework that ensures transparency, accountability, and protection of fundamental human rights.

Keywords: *Predictive Policing, Artificial Intelligence, Insecurity, Nigeria, Crime Prevention, Security, Algorithmic Governance, AI Ethics.*

INTRODUCTION

Nigeria continues to experience persistent and complex security challenges that have significantly affected national stability, socio-economic development, and public trust in law enforcement institutions. These challenges include insurgency in the North-East, banditry and mass abductions in the North-West, farmer–herder conflicts in the North-Central, and rising cases of kidnapping, armed robbery, cultism, and cybercrime in urban centers such as Lagos, Abuja, Oyo, and Kwara States. These overlapping security threats have placed enormous pressure on conventional policing strategies, which are often reactive rather than preventive in nature (Iwuoha & Aniche, 2022; Roberts et al., 2023). In response to these evolving security conditions, there is growing global and



national interest in using advanced technologies to strengthen law enforcement capacity. Among these innovations, artificial intelligence (AI)-driven predictive policing has emerged as a significant approach. Predictive policing applies machine learning algorithms, data analytics, and statistical modelling to identify patterns in crime data and forecast potential crime hotspots, enabling proactive law enforcement responses (Brayne & Christin, 2021; Ferguson, 2017). This approach is intended to improve resource allocation and enhance crime prevention strategies.

Globally, predictive policing systems and AI-based surveillance technologies have been deployed in several countries. In the United States, predictive crime mapping systems such as data-driven policing models have been used to guide patrol deployment (Ferguson, 2017). In the United Kingdom, facial recognition and data analytics support operational policing, although concerns about privacy and proportionality have been raised (House of Commons Library, 2020). In China, large-scale AI surveillance systems integrated into smart city infrastructures are used for real-time monitoring and population management (Qiang, 2019). Similarly, countries such as India, the United Arab Emirates, Kenya, Rwanda, and South Africa are increasingly adopting AI-enabled security systems for urban safety and crime prevention (Ahmed & Al-Khoury, 2020; Roberts et al., 2023). However, these developments have generated global debates on algorithmic bias, privacy violations, transparency, and accountability (Zavaršnik, 2021; Brayne & Christin, 2021).

Despite these global advancements, the adoption of predictive policing in Nigeria remains limited and fragmented. While technologies such as CCTV surveillance systems, biometric databases, and digital monitoring platforms exist, they are not yet integrated into a comprehensive national predictive policing framework. Furthermore, Nigeria's security environment is characterized by institutional weaknesses, limited data infrastructure, and trust deficits between citizens and law enforcement agencies, all of which may affect the effectiveness of AI-based policing systems (Iwuoha & Aniche, 2022). Existing literature on predictive policing is largely dominated by studies from developed countries, with relatively limited attention given to developing countries such as Nigeria. Most available studies focus on technical performance or general surveillance systems, with insufficient analysis of how predictive policing interacts with Nigeria's legal framework, governance structure, and socio-political realities (Chiemela & Obiora, 2023; Roberts et al., 2023). This creates a significant research gap, particularly in understanding whether such systems can be responsibly deployed in environments with weak regulatory oversight and existing concerns about policing accountability.

Against this background, this study examines the role of AI-driven predictive policing in addressing insecurity in Nigeria. It critically explores its potential contributions to crime prevention, while also assessing its limitations, risks, and governance implications within the Nigerian context. The study further situates Nigeria's experience within global and African comparative perspectives to provide a more balanced understanding of the opportunities and challenges associated with predictive policing technologies.



LITERATURE REVIEW

Conceptual Overview of Predictive Policing

Predictive policing refers to the use of data analytics, machine learning algorithms, and statistical modelling to forecast where crimes are likely to occur or who may commit them, enabling proactive rather than reactive law enforcement responses. Ferguson (2017) identifies two broad categories: place-based prediction, which focuses on geographic crime hotspots, and person-based prediction, which targets individuals deemed to be at elevated risk. While both approaches have demonstrated operational utility in various contexts, they have also attracted significant scholarly criticism regarding their reliability, fairness, and governance implications (Brayne & Christin, 2021; Zavaršnik, 2021).

A recurring concern in the literature is algorithmic bias, where predictive systems trained on historical crime data reproduce and amplify pre-existing racial and spatial inequalities. Lum and Isaac (2016) demonstrate that systems trained on arrest data tend to concentrate future policing activity in already over-policed communities, creating self-reinforcing feedback loops. Scholars have also raised concerns about transparency, as many predictive policing tools operate as commercial "black boxes," preventing meaningful external audit (Zavaršnik, 2021). Brayne and Christin (2021) further document institutional resistance among police personnel who feel that algorithmic outputs undermine professional discretion, a pattern consistent with broader research on occupational policing culture showing resistance to practices that increase the visibility of police conduct to external scrutiny (Loftus, Goold, & Mac Giollabhui, 2022).

More recently, the literature has broadened to examine generative AI applications in policing, including natural language processing for threat detection and large language models for intelligence synthesis. These developments pose new governance challenges for accountability, data minimization, and human oversight that existing regulatory frameworks have not yet fully addressed (European Parliament, 2024). The EU Artificial Intelligence Act (2024) is the most comprehensive regulatory response to date, classifying high-risk AI uses in law enforcement and mandating transparency, human oversight, and fundamental rights impact assessments before deployment. Similarly, the UNESCO Recommendation on the Ethics of AI (2021) and the OECD AI Principles (2019) set international normative benchmarks for responsible AI governance that are increasingly cited in African AI policy discussions.

Nigerian Legal and AI Governance Context

A significant gap in the existing literature on predictive policing in Nigeria is the limited engagement with domestic legal and governance frameworks. The Nigeria Data Protection Act 2023 (NDPA) establishes principles for lawful data processing, including purpose limitation, data minimization, and the rights of data subjects, provisions directly relevant to the operation of AI-based policing systems that collect and process large volumes of personal data. However, the Act's implementation remains nascent, and specific provisions governing law enforcement data processing have not yet been developed.

The Cybercrime (Prohibition, Prevention, etc.) Act 2015 further regulates electronic surveillance and interception of communications, with implications for data collection practices underpinning



predictive policing systems. Constitutional protections under Section 37 of the Constitution of the Federal Republic of Nigeria 1999 (as amended), which guarantees the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications, are directly relevant to AI-driven policing and surveillance systems (Chiemela & Obiora, 2023). Furthermore, Nigeria's National AI Policy (2024), developed under the National Information Technology Development Agency, signals an emerging institutional commitment to responsible AI development, though specific provisions for AI use in law enforcement remain limited. These frameworks collectively underscore both the legal basis for, and the regulatory constraints on, the deployment of predictive policing technologies in Nigeria.

Nigeria's Security Landscape and the Case for Predictive Policing

Nigeria's security landscape combines insurgency in the North-East, banditry and mass abductions in the North-West, farmer-herder conflict in the North-Central, and urban crime including kidnapping, armed robbery, and cybercrime, threats that studies attribute to governance deficits, weak intelligence systems, and limited state presence rather than to any single cause (International Crisis Group, 2023; UNDP, 2021). These threat types differ sharply in their susceptibility to predictive policing intervention. Place-based crime mapping, the approach with the strongest evidence base elsewhere (Ferguson, 2017), is best suited to spatially concentrated urban crime such as armed robbery and cult-related violence, where historical incident data and fixed infrastructure already exist (CLEEN Foundation, 2022; UNODC, 2021). It is far less suited to insurgency and banditry, which involve mobile, loosely networked armed groups operating across forested terrain in Zamfara, Katsina, Sokoto, and Kaduna States and forming localised "criminal governance systems" that evade fixed-point surveillance (International Crisis Group, 2022; SBM Intelligence, 2023; Premium Times, 2023). Boko Haram and ISWAP attacks on civilians, security personnel, and schools in Borno, Yobe, and Adamawa States, including the Chibok (2014), Dapchi (2018), and Kankara (2020) abductions, similarly reflect a security problem rooted in territorial control and weak state presence rather than the kind of recurring, mappable street crime predictive systems are designed to forecast (UNICEF, 2022a; ACLED, 2023; Nigeria Security Tracker, 2024).

These overlapping threats carry consequences extending well beyond physical violence, including disrupted schooling and rising dropout rates (UNICEF, 2022b), psychological trauma and weakened social cohesion (UNDP, 2021), economic decline through disrupted agriculture and trade (World Bank, 2023), large-scale internal displacement of affected communities (IDMC, 2022), heightened humanitarian needs requiring sustained international response (OCHA, 2023), and eroded public trust in state security institutions (Amnesty International, 2021). This combination of severity and institutional distrust creates a paradox for predictive policing in Nigeria: the same instability that makes proactive, intelligence-led tools attractive in principle is also what undermines the preconditions, reliable crime data, stable territorial control, and public cooperation with police that such tools require to function as intended. Whether predictive policing succeeds or fails in Nigeria, therefore, depends less on the technology itself than on which categories of insecurity it is applied to, and on whether data infrastructure and institutional trust are built up alongside its deployment, themes this study returns to in the Findings and Discussion section below.



International and Comparative Perspectives

The literature on predictive policing is shaped by several ongoing debates, and a major concern is algorithmic bias, where predictive systems replicate inequalities present in historical data, leading to disproportionate targeting of certain communities (Lum & Isaac, 2016; Brayne & Christin, 2021). Another major issue is transparency, as many predictive policing systems operate as "black boxes," making it difficult to evaluate how decisions are generated. Privacy and civil liberties also remain central concerns, particularly in contexts where legal frameworks have not kept pace with technological advancement. Scholars emphasize that while predictive policing may enhance efficiency, it risks undermining fundamental rights if not properly regulated (Zavaršnik, 2021). Additionally, issues of accountability arise when algorithmic outputs influence policing decisions without clear human oversight mechanisms. Overall, the literature suggests a dual reality: predictive policing offers significant potential for improving security operations, but it simultaneously introduces complex ethical, legal, and governance challenges that are especially pronounced in developing contexts such as Nigeria.

Country-level evidence illustrates this duality. In the United States, hotspot mapping and data-driven patrol deployment improved resource allocation but reinforced racial and spatial bias when built on historical arrest data (Ferguson, 2017; Lum & Isaac, 2016). In the United Kingdom, facial recognition and predictive analytics have raised proportionality and civil liberties concerns despite operational gains (House of Commons Library, 2020), while China's large-scale AI surveillance infrastructure demonstrates substantial technical capacity alongside limited transparency (Qiang, 2019). India, the United Arab Emirates, Kenya, Rwanda, and South Africa are integrating similar tools into urban security frameworks, generally through partnerships with foreign technology providers rather than domestically developed systems (Ahmed & Al-Khouri, 2020; Kumar & Gupta, 2021; Roberts et al., 2023). Across these cases, technology adoption without corresponding governance reform has consistently produced accountability deficits, a lesson with direct relevance for Nigeria given the institutional weaknesses and public distrust already noted in its own surveillance landscape, which includes CCTV networks and the Electronic Intelligent Monitoring Operational Platform (EIMOP) but lacks an integrated predictive policing infrastructure (Iwuoha & Aniche, 2022; Chiemela & Obiora, 2023).

THEORETICAL FRAMEWORK

This study is anchored on three complementary theoretical perspectives: Foucault's theory of surveillance and disciplinary power, the emerging concept of algorithmic governance, and AI ethics frameworks.

Foucauldian Surveillance Theory

Michel Foucault's concept of the panopticon explains how modern societies regulate behaviour through the perception of constant monitoring. In the context of digital governance, this framework applies to data-driven technologies, artificial intelligence, and algorithmic systems that function as new forms of surveillance power (Foucault, 1977). Predictive policing systems, which rely on data collection, pattern recognition, and behavioural prediction, operate similarly to the panoptic model by enabling authorities to monitor populations through digital traces and algorithmic



profiling. In Nigeria's policing environment, where concerns about accountability and abuse of power are well-documented, the introduction of AI-driven predictive policing may strengthen state surveillance capacity while also intensifying existing power imbalances if not properly regulated.

Algorithmic Governance

Beyond Foucault, this study engages with the concept of algorithmic governance, which refers to the increasing use of automated computational systems to make or inform public decisions. Algorithmic governance scholars argue that the delegation of decision-making authority to automated systems raises fundamental questions about democratic accountability, procedural fairness, and the visibility of power (Zavaršnik, 2021). In the policing context, when risk assessments are generated by machine learning models rather than human officers, traditional accountability mechanisms such as judicial review and community oversight may become inadequate. This is particularly relevant in Nigeria, where institutional oversight of policing is already constrained.

This concern connects to the broader phenomenon of digital authoritarianism, in which governments use data-driven surveillance and algorithmic profiling to consolidate political control and suppress dissent under the guise of security provision (Zuboff, 2019). While predictive policing in Nigeria is framed primarily as a crime-prevention tool, its core mechanisms, mass data collection, behavioural profiling, and automated risk classification, are the same mechanisms that enable digital authoritarian practices elsewhere. This dual-use risk is particularly salient in a context such as Nigeria's, where institutional checks on executive and security-sector power remain comparatively weak, making robust algorithmic governance not merely a technical safeguard but a political necessity.

AI Ethics Frameworks

International AI ethics frameworks, including the UNESCO Recommendation on the Ethics of AI (2021) and the OECD AI Principles (2019), provide a normative foundation for evaluating the responsible deployment of AI in law enforcement. These frameworks emphasize transparency, explainability, human oversight, non-discrimination, and protection of fundamental rights as core requirements for ethical AI systems. The EU AI Act (2024) operationalises these principles through binding legal requirements for high-risk AI systems, including those used in law enforcement. This study uses these frameworks to critically assess the governance gap between Nigeria's current legal infrastructure and the requirements for responsible predictive policing deployment.

METHODOLOGY

This study adopts a qualitative research design to examine the role of AI-driven predictive policing in addressing insecurity in Nigeria. The qualitative approach is appropriate because the study focuses on interpreting policy developments, governance frameworks, legal structures, and the socio-technical implications of predictive policing rather than testing numerical relationships or statistical hypotheses.



Search Strategy

Data for the study were collected through a systematic review of scholarly literature, policy documents, and institutional reports published between 2015 and 2026. The literature was sourced from reputable academic databases, including Scopus, Web of Science, Google Scholar, and African Journals Online (AJOL), as well as relevant reports from international organisations and government agencies addressing artificial intelligence, surveillance systems, and criminal justice governance. Search terms used included: "predictive policing," "AI policing Nigeria," "algorithmic surveillance Africa," "AI governance developing countries," "surveillance and human rights Nigeria," and combinations thereof.

Screening Procedure and Inclusion/Exclusion Criteria

To ensure rigour and relevance, clear inclusion and exclusion criteria guided the selection of materials. Studies were included if they focused on predictive policing, artificial intelligence applications in security, algorithmic governance, or surveillance technologies, and were published within the specified timeframe. Only peer-reviewed journal articles, official policy documents, and credible institutional reports were considered. Studies were excluded if they were unrelated to AI-enabled policing systems, lacked empirical or policy relevance, or were purely opinion-based without scholarly or institutional grounding. An initial search returned over 200 results; after title and abstract screening, 68 sources were assessed for full-text eligibility; 42 peer-reviewed articles and institutional reports were ultimately included in the review.

Review Flow

The review proceeded in three stages: (1) identification and retrieval of sources from databases using defined search terms; (2) screening against inclusion/exclusion criteria at title/abstract and full-text levels; and (3) extraction and thematic synthesis of relevant content. The search process initially identified more than 200 records. Following title and abstract screening, 68 studies were retained for full-text assessment, of which 42 met the inclusion criteria and were included in the final review. This staged process enhances transparency and replicability in accordance with established systematic review standards.

Comparative Framework

The comparative dimension of the study is based on the selection of Kenya, Rwanda, and South Africa as reference cases. These countries were chosen due to their increasing adoption of digital surveillance technologies and their relevance within the African security governance landscape. They provide meaningful comparative insight because they share similar socio-political and institutional characteristics with Nigeria, particularly in relation to governance capacity, security challenges, and ongoing digital transformation in public safety systems.

Data Analysis

The data collected were analysed using thematic analysis, which involved identifying, categorising, and interpreting recurring patterns across the literature. Through this process, key themes such as predictive policing efficiency, algorithmic bias, surveillance governance, legal and



ethical concerns, and institutional capacity were extracted and synthesised to provide a coherent analytical framework. A comparative analytical approach was also employed to examine similarities and differences in how predictive policing and AI-enabled surveillance systems are being implemented across different jurisdictions.

FINDINGS AND DISCUSSION

This section presents the key findings of the systematic review, organised thematically. Each theme reflects a pattern identified across multiple sources and is discussed in relation to both global evidence and the specific Nigerian context.

Theme 1: Potential of Predictive Policing for Security Enhancement

The review finds that, where data quality and institutional capacity are adequate, predictive policing systems can improve security operations through enhanced crime mapping, early warning systems, and more efficient resource allocation. Ferguson (2017) documents measurable reductions in response times in US jurisdictions using data-driven patrol deployment. In African contexts, Roberts et al. (2023) document improvements in urban crime response in South African cities following the integration of digital surveillance tools. These findings suggest that, in principle, predictive policing could address aspects of Nigeria's security deficit, particularly in improving intelligence-led resource deployment in urban centres.

However, the evidence also consistently shows that these benefits are context-dependent. They require high-quality, comprehensive crime data, well-trained personnel, and robust oversight mechanisms, conditions that are currently underdeveloped in Nigeria. Without these prerequisites, predictive policing systems risk producing unreliable outputs that may misdirect limited policing resources. A more critical examination of the conditions underpinning success in jurisdictions such as the United States and United Kingdom reveals a striking contrast with Nigeria's institutional realities. Predictive policing has produced measurable gains in these contexts precisely because several enabling conditions converge: decades of systematically digitised and geospatially coded crime records that provide high-quality training data; well-resourced and technologically literate police forces capable of interpreting and interrogating algorithmic outputs; independent judicial and civilian oversight bodies that constrain misuse; and, critically, a foundational level of public trust in law enforcement that encourages community reporting and data sharing (Ferguson, 2017; House of Commons Library, 2020). In Nigeria, each of these conditions is either absent or severely underdeveloped. Crime data collection remains fragmented and inconsistent across the thirty-six states, with no unified national crime database equivalent to those that underpin US predictive systems (CLEEN Foundation, 2022; Iwuoha & Aniche, 2022). Police personnel capacity for data-driven analysis is limited by chronic underfunding and inadequate training (International Crisis Group, 2023). Independent oversight of the Nigeria Police Force remains structurally weak, and public trust, already eroded by the EndSARS crisis and documented abuses by units such as SARS, cannot be assumed (Amnesty International, 2021). The implication is not that predictive policing can never be effective in Nigeria; rather, its successful, legitimate, and sustainable deployment depends on first addressing the underlying structural deficits within the country's security and



governance systems. This sequencing logic is crucial, yet it has been insufficiently acknowledged in much of the existing advocacy for technology-driven security reform.

Theme 2: Algorithmic Bias and Structural Inequalities

A consistent finding across the reviewed literature is that predictive policing systems trained on historical data reproduce and amplify pre-existing biases. Lum and Isaac (2016) demonstrate mathematically that systems trained on arrest records will systematically over-predict crime in already over-policed communities, creating feedback loops that entrench spatial and racial inequalities. Brayne and Christin (2021) further document how algorithmic outputs can displace professional discretion without improving decision quality. In the Nigerian context, these risks are particularly acute because historical policing data reflect patterns of abuse documented in multiple human rights reports, particularly the activities of units such as the disbanded Special Anti-Robbery Squad (SARS). Deploying predictive systems trained on such data could systematically target the same communities and demographics that have historically been subject to police abuse, further undermining public trust.

Theme 3: Surveillance Governance and Legal Gaps

The review identifies a substantial governance gap between the demands of responsible deployment of predictive policing and Nigeria's current regulatory infrastructure. While the Nigeria Data Protection Act 2023 establishes foundational principles for lawful data processing, it does not specifically address law enforcement data collection or the use of AI-generated risk scores in policing decisions. The Cybercrime Act 2015 regulates certain forms of electronic surveillance but predates the emergence of AI-powered policing tools. International benchmarks, including the EU AI Act (2024) and the UNESCO AI Ethics Framework (2021), require that high-risk AI systems in law enforcement be subject to fundamental rights impact assessments, transparency obligations, and human oversight requirements. Nigeria's current frameworks do not yet incorporate these standards, creating significant regulatory risk if predictive policing is deployed without prior legislative reform.

Theme 4: Institutional Capacity and Public Trust Deficits

The review consistently finds that technical deployment of predictive policing without corresponding institutional reform is unlikely to produce legitimate or effective outcomes. Studies from African contexts, including Kenya and South Africa, show that surveillance technology adoption without accountability reform can entrench existing patterns of over-policing and selective enforcement (Roberts et al., 2023). In Nigeria, trust deficits between communities and police are well-documented, intensified by experiences such as the EndSARS movement, which highlighted patterns of police brutality and impunity (Amnesty International, 2021; Iwuoha & Aniche, 2022). Introducing AI-based policing systems in this environment, without first addressing institutional accountability, risks amplifying existing tensions and reducing rather than improving community cooperation with law enforcement.

LIMITATIONS



This study acknowledges several limitations that should inform the interpretation of its findings. First, the study relies entirely on secondary data, as no primary empirical data were collected from Nigerian policing institutions or communities. This limits the depth of insight into implementation realities on the ground. Second, there is a general scarcity of African-specific predictive policing research, which means that several findings are extrapolated from global and especially Western contexts where institutional conditions differ significantly. Third, the reliance on published academic literature introduces potential publication bias, as studies reporting null or negative outcomes may be underrepresented. Fourth, the rapidly evolving nature of AI technology means that some reviewed studies may not fully reflect the current capabilities of available systems. Future research should prioritise primary empirical investigation within Nigerian policing contexts and engage directly with law enforcement institutions and affected communities.

POLICY IMPLICATIONS

The findings of this study have several important policy implications for Nigeria's approach to AI-driven policing. First, legislative reform is urgently needed to establish a clear regulatory framework governing AI use in law enforcement. This framework should draw on the Nigeria Data Protection Act 2023, constitutional privacy provisions, and international standards such as the EU AI Act and UNESCO AI Ethics Framework, and should specifically require fundamental rights impact assessments before deployment of any predictive policing system. Second, Nigeria's National AI Policy should be expanded to include binding provisions for law enforcement AI, including transparency requirements, audit mechanisms, and data governance standards. Third, institutional capacity building within the Nigerian Police Force is necessary to ensure that personnel can critically evaluate and appropriately apply algorithmic outputs rather than treating them as determinative. Fourth, independent oversight mechanisms should be established or strengthened to provide civilian oversight of AI-based policing tools, consistent with existing constitutional principles of accountability.

CONCLUSION

AI-driven predictive policing offers potential benefits for improving security in Nigeria through better crime detection, early warning systems, and more efficient use of limited policing resources. However, the systematic review conducted in this study demonstrates that these benefits are heavily contingent on data quality, institutional capacity, and strong governance structures that are currently underdeveloped in the Nigerian context. The study finds that predictive policing may introduce risks such as algorithmic bias, privacy violations, and the reinforcement of existing inequalities within policing systems, risks that are intensified in Nigeria by weak regulatory frameworks and documented trust deficits in law enforcement. Critically, Nigeria's existing legal frameworks, including the Data Protection Act 2023, Cybercrime Act 2015, and constitutional privacy provisions, do not yet provide adequate governance for AI-based policing systems when measured against international benchmarks such as the EU AI Act (2024) and UNESCO AI Ethics Framework (2021). The study concludes that any deployment of predictive policing in Nigeria must be preceded by legislative reform, institutional accountability improvements, and the establishment of robust independent oversight. Predictive policing should function only as a



decision-support tool within broader policing reforms, not as an autonomous or determinative system.

RECOMMENDATIONS

To ensure the responsible use of AI-driven predictive policing in Nigeria, the following policy measures are recommended:

1. Nigeria should enact specific legislation governing AI use in law enforcement, incorporating fundamental rights impact assessment requirements, transparency obligations, and human oversight mandates, drawing on the EU AI Act (2024) and Nigeria Data Protection Act 2023 as reference frameworks.
2. Security agencies should be required to conduct human rights impact assessments before deploying predictive policing systems, in line with constitutional provisions and international human rights standards.
3. An independent civilian oversight body should be established or strengthened to regularly audit AI-based policing tools, investigate cases of misuse or discriminatory profiling, and ensure public accountability.
4. The Nigeria National AI Policy should be updated to include binding provisions for law enforcement AI, with clear standards for data governance, model transparency, and accountability.
5. Predictive policing systems should undergo controlled pilot testing and independent evaluation before any large-scale deployment, with results made publicly available.
6. Institutional capacity building within the Nigeria Police Force should accompany any technological deployment, ensuring that personnel are equipped to critically evaluate algorithmic outputs and maintain human oversight of AI-driven decisions.
7. The use of surveillance technologies within educational institutions should be strictly regulated to protect academic freedom, freedom of expression, and student rights.

REFERENCES

- ACLED. (2023). *Armed conflict location & event data project: Nigeria country report*. ACLED Data. <https://acleddata.com>
- Ahmed, E., & Al-Khouri, A. M. (2020). Smart government and artificial intelligence in the United Arab Emirates: A policy perspective. *Journal of Information Technology & Politics*. <https://doi.org/10.1080/19331681.2020.1710604>.
- Amnesty International. (2021). *Nigeria: Time to end impunity for human rights violations*. Amnesty International. <https://www.amnesty.org>.
- Brayne, S., & Christin, A. (2021). Technologies of crime prediction: The reception of algorithms in policing and criminal courts. *Social Problems*. <https://doi.org/10.1093/socpro/spaa004>



- Chiemela, C., & Obiora, K. (2023). Artificial intelligence and constitutional rights in Nigeria: Interrogating the legal frameworks for AI-driven policing. *African Journal of Law and Technology*. <https://africanjournaloflawtech.org>.
- CLEEN Foundation. (2022). *National crime and safety survey report*. CLEEN Foundation. <https://cleenfoundation.org>.
- European Parliament. (2024). *Regulation (EU) 2024/1689 (Artificial Intelligence Act)*. Official Journal of the European Union.
- Ferguson, A. G. (2017). *The rise of big data policing: Surveillance, race, and the future of law enforcement*. NYU Press.
- Foucault, M. (1977). *Discipline and punish: The birth of the prison*. Pantheon Books.
- House of Commons Library. (2020). *Facial recognition technology in policing in the UK*. UK Parliament.
- IDMC (Internal Displacement Monitoring Centre). (2022). *Global report on internal displacement*. IDMC. <https://www.internal-displacement.org>.
- International Crisis Group. (2022). *Violence in Nigeria's North-West: Rising insecurity and banditry*. International Crisis Group. <https://www.crisisgroup.org>.
- International Crisis Group. (2023). *Nigeria's insecurity crisis: Drivers and responses*. International Crisis Group. <https://www.crisisgroup.org>.
- Iwuoha, V. C., & Aniche, E. T. (2022). Protests and blood on the streets: Repressive state, police brutality and #EndSARS protest in Nigeria. *Security Journal*. <https://doi.org/10.1057/s41284-021-00316-z>.
- Kumar, V., & Gupta, M. (2021). Artificial intelligence in Indian policing: Opportunities and challenges. *Journal of Asian Security Studies*.
- Loftus, B., Goold, B., & Mac Giollabhui, S. (2022). From a visible spectacle to an invisible presence: The working culture of covert policing. *British Journal of Criminology*. <https://doi.org/10.1093/bjc/azab094>
- Lum, K., & Isaac, W. (2016). To predict and serve? *Significance*. <https://doi.org/10.1111/j.1740-9713.2016.00960.x>.
- National Information Technology Development Agency (NITDA). (2024). *Nigeria National AI Policy*. Federal Republic of Nigeria.
- Nigeria Security Tracker. (2024). *Violence and insecurity trends in Nigeria*. Council on Foreign Relations. <https://www.cfr.org/nigeria>.
- OCHA (United Nations Office for the Coordination of Humanitarian Affairs). (2023). *Nigeria humanitarian needs overview*. OCHA. <https://www.unocha.org>



- OECD. (2019). *Recommendation of the Council on Artificial Intelligence*. OECD. <https://oecd.ai/en/ai-principles>.
- Premium Times. (2023). *Banditry and kidnapping in North-West Nigeria*. Premium Times. <https://www.premiumtimesng.com>.
- Qiang, X. (2019). The road to digital unfreedom: President Xi's surveillance state. *Journal of Democracy*.
- Roberts, T., Marchetti, N., Bhatt, M., Allen, R., Tilsley, P., Maweu, J. M., & Spires, H. (2023). *Mapping the supply of surveillance technologies to Africa: Case studies from Nigeria, Ghana, Morocco, Malawi, and Zambia*. Institute of Development Studies. <https://doi.org/10.19088/IDS.2023.027>
- SBM Intelligence. (2023). *Nigeria security risk report*. SBM Intelligence. <https://sbmintelligence.com>
- UNDP. (2021). *Human security and development report: Nigeria context*. UNDP. <https://www.undp.org>.
- UNESCO. (2021). *Recommendation on the Ethics of Artificial Intelligence*. UNESCO Publishing.
- UNICEF. (2022a). *Education under attack: Nigeria country profile*. UNICEF. <https://www.unicef.org>.
- UNICEF. (2022b). *Education under attack 2022: Nigeria country report*. UNICEF Publications. <https://www.unicef.org>
- UNODC. (2021). *Crime and development in Nigeria*. UNODC. <https://www.unodc.org>
- World Bank. (2023). *Nigeria development update: Security and economic impact*. World Bank. <https://www.worldbank.org>.
- Zavaršnik, A. (2021). Algorithmic justice: Algorithms and big data in criminal justice settings. *European Journal of Criminology*. <https://doi.org/10.1177/1477370819876762>
- Zuboff, S. (2019). *The age of surveillance capitalism*. Public Affairs.