ETHICAL AND LEGAL IMPLICATIONS OF AI-DRIVEN ANTI-CORRUPTION TECHNOLOGIES IN DEVELOPING DEMOCRACIES

Ember Yange

Email: emberyange@gmail.com

Cite this article:

Ember Yange (2026), Ethical and Legal Implications of AI-Driven Anti-Corruption Technologies in Developing Democracies. African Journal of Law, Political Research and Administration 9(1), 100-118. DOI: 10.52589/AJLPRA-LX5SFQ4O

Manuscript History

Received: 10 Mar 2026

Accepted: 7 Apr 2026

Published: 17 Jun 2026

ABSTRACT: *This study explores the potential of Artificial Intelligence (AI)-driven procurement monitoring to enhance transparency, accountability, and fraud detection in public procurement systems within developing democracies. It employs a comparative policy and literature-based analysis of global AI governance practices and emerging digital oversight models, with a focus on how machine learning concepts such as anomaly detection and predictive risk scoring are applied in procurement oversight frameworks. The findings suggest that AI has strong potential to support procurement integrity by identifying risk patterns, improving audit prioritization, and enhancing transparency through data-driven decision-support systems. However, its effectiveness is highly dependent on institutional readiness, data governance quality, and regulatory frameworks that ensure accountability and fairness. Despite these advantages, significant challenges remain, including poor data quality, algorithmic bias, limited institutional capacity, political resistance, and concerns regarding explainability and transparency. These challenges highlight that AI should not be viewed as a fully automated enforcement tool, but rather as a decision-support mechanism that complements human oversight. Effective adoption therefore requires complementary reforms in data governance, institutional capacity building, open data standards, and the integration of AI-generated insights into existing accountability structures. Future research should focus on context-specific implementation strategies, evaluate the real-world impact of AI-supported procurement monitoring on corruption reduction, and develop governance frameworks that mitigate algorithmic bias while ensuring transparency, accountability, and institutional trust in developing democracies.*

KEYWORDS: Artificial Intelligence, Public Procurement, Corruption, Developing Democracies, Transparency.

INTRODUCTION

Artificial intelligence (AI) has rapidly transitioned from theoretical innovation into a practical tool of governance, offering new capabilities to detect, prevent, and respond to corruption. AI-driven anti-corruption technologies (ACTs), including machine learning, predictive analytics, and natural language processing, are increasingly being adopted by governments and oversight institutions to strengthen transparency and accountability in public administration. These systems are capable of detecting irregular financial patterns, flagging high-risk contracts, and supporting investigative processes more efficiently than traditional manual approaches (Ezeji, 2024). However, as these tools expand into the public sector—particularly in emerging and resource-constrained governance systems—they raise complex ethical and legal questions that require careful scrutiny.

One of the primary ethical concerns is fairness and algorithmic bias. Because AI systems are trained on historical datasets, they may reproduce existing inequalities or reflect embedded patterns of corruption within those datasets, thereby reinforcing systemic bias if not properly audited and corrected (Resimić et al., 2025). Additionally, the "black box" nature of many machine learning models limits interpretability, making it difficult for citizens, auditors, and legal institutions to understand how decisions are generated. This lack of explainability can weaken institutional trust and undermine the legitimacy of anti-corruption interventions, even when such systems improve efficiency (Transparency International, 2025).

Unlike jurisdictions such as the European Union, where the AI Act provides a structured risk-based regulatory framework, legal systems in emerging governance contexts such as Nigeria and Brazil continue to face significant regulatory gaps in the deployment of AI for public accountability and corruption monitoring. In these settings, AI technologies are often introduced faster than corresponding legal safeguards, resulting in a mismatch between technological capability and institutional oversight. This creates uncertainty around accountability when algorithmic systems produce errors, misclassify entities, or negatively affect reputational integrity (Hakimi et al., 2025). In Nigeria, for example, AI-assisted governance tools are still largely governed through general data protection and public service rules rather than AI-specific legislation, while Brazil continues to rely on evolving draft frameworks for algorithmic governance.

In contexts where rule-of-law institutions are still developing, this regulatory lag can create additional risks, including potential misuse of AI-generated outputs by officials without sufficient transparency or oversight mechanisms. As a result, while AI-driven anti-corruption systems hold significant promise, their effectiveness ultimately depends on the existence of strong legal safeguards, institutional capacity, and enforceable accountability structures that ensure responsible deployment (Ayibam, 2025).

At the same time, the potential benefits of AI in anti-corruption efforts should not be overlooked. Tools that can process large datasets to identify risky patterns or anomalies provide governments and civil society with unprecedented analytical capacity (OECD, 2024). For example, predictive analytics can help allocate limited investigative resources more effectively, while automated audits of public procurement records can uncover irregularities that previously went unnoticed. These applications illustrate how technology can complement human judgment and strengthen institutional capacity when implemented with safeguards.

Article DOI: 10.52589/AJLPRA-LX5SFQ4O
DOI URL: https://doi.org/10.52589/AJLPRA-LX5SFQ4O

Despite these advantages, the ethical implications of deploying AI in developing democracies go beyond technical performance. Questions about privacy, consent, and surveillance emerge when government systems begin to analyze personal or financial data at scale. Citizens may feel their rights are compromised if AI tools are used without clear consent mechanisms or if data governance structures are weak (UNDP, 2025). Moreover, the risk that corrupt actors might manipulate AI systems themselves either to hide wrongdoing or to target political opponents adds another layer of complexity to the legal landscape.

Ultimately, the successful integration of AI-driven anti-corruption technologies in developing democracies depends on a balanced approach that embraces innovation while upholding democratic values, human rights, and legal protections. This includes building institutional capacity to govern AI, developing context-specific ethical guidelines, and ensuring meaningful public engagement in how these tools are adopted and overseen (OECD, 2025). By foregrounding ethical and legal considerations alongside technological promise, policymakers and stakeholders can work toward anti-corruption strategies that are both effective and aligned with the principles of democratic governance.

Statement of problem

Efforts to combat corruption in developing democracies are increasingly turning to artificial intelligence to monitor public spending, detect fraud, and improve transparency. However, a major paradox has emerged: technologies intended to reduce corruption are often deployed in environments with weak regulatory systems, limited institutional oversight, and inadequate legal safeguards. In many cases, AI systems are used to influence sensitive decisions involving investigations, reputations, and access to public resources without clear standards for accountability, transparency, or fairness. Consequently, tools designed to strengthen governance may instead create opportunities for bias, political manipulation, excessive surveillance, and new forms of injustice, especially when algorithms rely on incomplete or poorly governed data.

The absence of comprehensive legal and ethical frameworks governing the use of AI in anti-corruption initiatives further deepens this challenge. Issues relating to data privacy, due process, liability, and algorithmic transparency remain largely unresolved in many developing democracies, increasing the risk that AI-driven systems could undermine civil liberties, weaken public trust, and reinforce existing power imbalances rather than promote democratic accountability. The problem, therefore, is not simply the adoption of AI technologies, but the lack of effective governance structures capable of ensuring that such technologies operate responsibly, transparently, and in accordance with democratic principles.

Consequently, this study is guided by the following research questions:

i. How can the ethical and legal challenges associated with deploying AI-driven anti-corruption technologies in developing democracies be effectively identified and addressed?

ii. What policy and governance frameworks can be recommended to ensure that AI-driven anti-corruption technologies are used responsibly, transparently, and in alignment with democratic principles?

Article DOI: 10.52589/AJLPRA-LX5SFQ4O
DOI URL: https://doi.org/10.52589/AJLPRA-LX5SFQ4O

Artificial Intelligence (AI)

AI-driven anti-corruption technologies (ACTs) refer to the use of artificial intelligence systems, including machine learning and automated data analytics, to detect fraud, monitor public spending, identify suspicious transactions, and enhance transparency and accountability in governance processes (Li et al., 2023; Andersson et al., 2025). These technologies are increasingly being adopted in governance and public administration due to their ability to process large volumes of data, identify irregular patterns, and support oversight mechanisms in real time. However, their growing deployment has also raised significant concerns regarding transparency, accountability, bias, privacy, and democratic governance, particularly in developing democracies where regulatory and institutional safeguards remain weak. These concerns provide the basis for examining AI-driven anti-corruption technologies from a governance and theoretical perspective rather than from a purely technical standpoint.

THEORETICAL FRAMEWORK

Technology Governance Theory

This study is grounded in Dominique Foray's Technology Governance Theory (TGT) (2004), which posits that technological innovation is not inherently neutral, but must be actively guided through institutional frameworks, regulatory oversight, and ethical safeguards to achieve socially desirable outcomes. Within the context of developing democracies, the theory provides a useful analytical lens for understanding how the deployment of AI-driven anti-corruption technologies, despite their potential to improve transparency and efficiency, can also generate serious risks when introduced into weakly regulated governance environments. In areas such as public procurement, fraud detection, and financial monitoring, the absence of effective governance structures may enable algorithmic bias, political manipulation, privacy violations, and public mistrust, thereby undermining the democratic accountability these technologies are intended to strengthen.

Rather than viewing AI adoption as a purely technical solution to corruption, TGT shifts attention toward the institutional and ethical conditions necessary for responsible implementation. The theory therefore supports the central argument of this study that the effectiveness of AI-driven anti-corruption technologies depends not only on technological capability, but also on the existence of transparent legal frameworks, accountability mechanisms, and democratic oversight structures capable of regulating their use in developing democracies.

Article DOI: 10.52589/AJLPRA-LX5SFQ4O
DOI URL: https://doi.org/10.52589/AJLPRA-LX5SFQ4O

African Journal of Law, Political Research and Administration
ISSN: 2689-5102
Volume 9, Issue 1, 2026 (pp. 100-118)
www.abjournals.org

METHODOLOGY

This study adopts a qualitative-quantitative mixed methods design to investigate the ethical and legal implications of AI-driven anti-corruption technologies in developing democracies. The mixed approach is appropriate because AI anti-corruption tools involve both data-driven mechanisms requiring computational analysis of procurement and governance datasets and institutional and regulatory considerations, which require qualitative insights from policy, legal frameworks, and stakeholder perspectives. The quantitative component analyzes patterns of AI implementation, risk factors, and compliance outcomes, while the qualitative component explores governance challenges, legal interpretations, and ethical concerns in deploying such technologies.

Data Collection

Secondary data was sourced from official procurement records available through the Nigerian Bureau of Public Procurement (BPP), audit reports, and World Bank governance datasets. This was complemented by open-source contract award databases and relevant policy documents. For the qualitative dimension, data were collected through document analysis of government policy papers, regulatory frameworks, anti-corruption reports, and scholarly literature relating to AI governance and public procurement in developing democracies. This combination of quantitative and qualitative sources provided a broader understanding of both the operational use of AI-driven anti-corruption technologies and the governance challenges associated with their deployment.

Data Analysis

Quantitative data were analyzed using analytical and computational techniques, including logistic regression, anomaly detection, and clustering, to identify potential ethical and legal risks, such as algorithmic bias, non-compliance with regulatory standards, and lack of transparency in AI monitoring processes.

Model Specification

This study specifies an analytical model designed to assess the likelihood of procurement fraud in public contracts using logistic regression implemented in TensorFlow, with data stored and managed in MySQL. The model estimates the probability that a given procurement contract is fraudulent based on observable contract and firm-level characteristics. Logistic regression is appropriate because the dependent variable, fraud occurrence, is binary (fraudulent = 1, non-fraudulent = 0). The model predicts the probability that a contract is fraudulent using a set of independent variables, including contract value, number of bidders, award timeline, and firm ownership characteristics. These variables were selected because they reflect well-established risk indicators in procurement fraud literature, such as single-bid contracting, inflated pricing, non-competitive award processes, and collusive vendor behavior. MySQL was used to organize, query, and preprocess the procurement datasets, ensuring that the data fed into TensorFlow was clean, structured, and suitable for predictive modeling.

The functional form of the logistic regression model can be expressed as:

$$P(Fraud = 1) = 1 / (1 + e^{-(\beta 0 + \beta 1X1 + \beta 2X2 + \beta 3X3 + \beta 4X4)})$$

Where:

Article DOI: 10.52589/AJLPRA-LX5SFQ4O
DOI URL: https://doi.org/10.52589/AJLPRA-LX5SFQ4O

X1 = Contract value
X2 = Number of bidders
X3 = Award timeline (procurement duration or speed of award)
X4 = Firm ownership characteristics (e.g., related-party ownership, shell companies, or politically exposed connections)

The coefficients (β) represent the influence of each variable on the probability of procurement fraud. For instance, a positive coefficient for contract value suggests that higher-value contracts are associated with increased fraud risk, while a negative coefficient for the number of bidders implies that more competitive bidding reduces the likelihood of fraud. Similarly, shorter or unusually rapid award timelines may increase fraud probability, indicating possible procedural bypassing, whereas transparent ownership structures may reduce risk.

For qualitative analysis, thematic coding of procurement policy documents, anti-corruption statutes, and regulatory guidelines was conducted to identify recurring patterns, enforcement gaps, and legal ambiguities. These qualitative insights were then triangulated with quantitative results to provide a comprehensive understanding of procurement fraud risk factors and the effectiveness of data-driven anti-corruption monitoring systems.

The Rise of AI-Driven Anti-Corruption Tools

In the last few years, the integration of artificial intelligence into anti-corruption efforts has shifted from theoretical discussion to practical implementation. Governments and international organizations are increasingly experimenting with AI systems to strengthen transparency and accountability in public administration. For example, predictive analytics and machine-learning tools are now being used to analyze vast public procurement datasets, detect irregularities, and identify risks of fraud far more efficiently than traditional manual methods (OECD, 2025). These analytical capabilities allow oversight bodies to focus limited human resources on cases that exhibit the highest potential for corrupt marking a significant innovation in how corruption risk is managed globally.

The expansion of AI for anti-corruption work is not limited to analytical functions but also includes pioneering governance applications that challenge conventional bureaucracy. In 2025, Albania appointed an AI-powered digital assistant named Diella to support transparency in public procurement, symbolizing a bold step toward digitally managed oversight to reduce opportunities for bribery and influence (The Guardian, 2025; IndiaTimes, 2025). At the same time, enforcement agencies in various regions are adopting AI tools to support investigations by automating time-intensive document review and pattern recognition tasks. A recent OECD forum highlighted how AI is being combined with big data analytics to uncover bribery schemes and strengthen compliance workflows, indicating growing momentum in applying these technologies to real-world integrity challenges (OECD, 2025).

Applying these technologies to real-world integrity challenges, the Organisation for Economic Co-operation and Development has highlighted the growing role of artificial intelligence in strengthening public sector transparency, improving fraud detection, and enhancing procurement monitoring systems across member and partner countries (OECD, 2025).

Article DOI: 10.52589/AJLPRA-LX5SFQ4O
DOI URL: https://doi.org/10.52589/AJLPRA-LX5SFQ4O

Despite enthusiasm over their potential, AI-driven anti-corruption tools also introduce new complexities that require careful institutional and legal assessment. While these technologies offer unprecedented speed and large-scale data processing capabilities, their effectiveness depends heavily on data quality, institutional capacity, and strong ethical safeguards to ensure fairness, accountability, and transparency (Resimić et al., 2025). There are also concerns about overreliance on automated systems without sufficient human oversight, as well as the risk that strategic actors may manipulate AI-supported governance systems, potentially undermining institutional trust and creating new forms of algorithmic exploitation.

Recent developments such as Albania's AI-based public procurement assistant "Diella" have been discussed in policy and governance literature rather than journalistic reporting, with emphasis on its potential to reduce corruption risks through automated contract screening and transparency mechanisms (World Bank Governance Practice, 2025). However, scholars and policy analysts caution that such systems must be embedded within strong legal and institutional frameworks to prevent misuse, ensure auditability, and maintain public accountability (United Nations Development Programme, 2025). As AI's role in anti-corruption expands, balancing technological innovation with robust governance structures and enforceable legal safeguards remains essential to ensure responsible and sustainable adoption.

Legal Frameworks for Emerging Technologies

Legal frameworks for emerging technologies like artificial intelligence are rapidly evolving as governments and international bodies attempt to balance innovation with the protection of citizens' rights. One of the most influential legal responses has been the European Union's AI Act, which establishes a risk-based regulatory framework for artificial intelligence systems and introduces strict requirements for high-risk applications, including transparency, accountability, and human oversight (Veale & Borgesius, 2021). This landmark regulation is designed to ensure that AI development and deployment protect fundamental rights, prevent harm, and foster trustworthy technology, setting a precedent for global AI governance.

In addition to the EU's approach, national and regional frameworks are emerging with different priorities and strengths. For instance, South Korea's AI governance reforms focus on regulating high-impact AI systems through risk assessment requirements and safety reporting obligations, although concerns remain regarding enforcement capacity and gaps in individual protections (Calo, 2024). Similarly, India's AI governance direction emphasizes accountability, transparency, and ethical safeguards while attempting to create innovation-friendly legal structures ahead of full legislative adoption (Kumar & Bhatia, 2024). These examples show that legal frameworks are not only about restricting harmful practices but also about creating regulatory certainty that encourages responsible technological development.

International legal instruments are also playing a key role in shaping the governance landscape. In 2024, the Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law was adopted under the Council of Europe, committing member states to core principles such as transparency, non-discrimination, and accountability in AI systems and requiring human rights impact assessments (Hoffmann-Riem, 2024). Such treaties aim to harmonize legal standards across jurisdictions and provide guidance for emerging democracies that may lack standalone AI legislation, ensuring alignment with democratic values and fundamental freedoms.

Article DOI: 10.52589/AJLPRA-LX5SFQ4O
DOI URL: https://doi.org/10.52589/AJLPRA-LX5SFQ4O

Despite these advances, many developing democracies still rely primarily on existing laws such as data protection, cybercrime, and privacy statutes to regulate AI indirectly, which can leave significant gaps in addressing the unique challenges of emerging technologies (Crawford, 2024). For example, countries such as Kenya and South Africa are developing national AI strategies and strengthening data protection frameworks to address ethical and legal issues, but comprehensive AI-specific legislation remains in early stages, often without strong enforcement mechanisms (Zuboff, 2024). This uneven legal landscape underscores the need for more context-sensitive legal reform that integrates ethical safeguards, oversight mechanisms, and public accountability in governing emerging technologies.

AI in Public Procurement Monitoring

As governments seek to improve transparency and accountability in public procurement, AI-driven monitoring tools have become an important innovation in reducing opportunities for corruption and inefficiency. For example, Ukraine's *ProZorro* e-procurement system uses machine learning and advanced analytics to standardize classification codes, monitor procurement data in real time, and generate dashboards that help oversight bodies and civil society identify irregular trends and risk indicators (OECD, 2025). These analytical tools have been widely adopted, enabling tens of thousands of users to analyze procurement markets covering billions in public spending and contributing to significant cost savings through data-driven regulatory improvements.

In Brazil, the Comptroller General's Office developed *Alice*, an AI-powered system that continuously scans bids, contracts, and notices to detect irregularities and potential fraud in federal procurement processes. By automating large-scale audits and highlighting risk flags, Alice supports officials in prioritizing investigations and making informed decisions for oversight (OECD, 2025). Similarly, AI agents designed for procurement transparency can harmonize disparate tender documents and use natural language understanding to parse proposals, extract key criteria, and perform automated compliance checks (Guru Startups Market Intelligence, 2025). These tools extend beyond simple automation by flagging anomalies such as price fluctuations or suspicious bidding patterns that may indicate collusion or corruption, thus strengthening preventive capabilities.

While the adoption of AI in procurement monitoring shows promise in enhancing efficiency and revealing hidden risks, researchers note ongoing challenges around data quality, ethical safeguards, and institutional capacity to interpret algorithmic outputs. AI systems must be paired with robust governance frameworks to prevent bias and ensure that flagged irregularities lead to fair and legally defensible actions rather than false accusations. Nonetheless, when implemented with appropriate oversight and transparency, AI-driven monitoring tools offer powerful mechanisms to improve integrity in government contracting and promote public trust.

Increased Transparency and Detection Speed of AI

Artificial intelligence has helped improve transparency in governance by making complex government data more accessible and easier to understand. Instead of relying on manual audits and paper records that can take days or weeks to review, AI systems can rapidly process large volumes of financial and administrative information. For example, machine learning and natural language processing tools can convert handwritten tax returns into digital

Article DOI: 10.52589/AJLPRA-LX5SFQ4O
DOI URL: https://doi.org/10.52589/AJLPRA-LX5SFQ4O

text, classify content into meaningful categories, and flag anomalies that may indicate fraud or misuse of funds much faster than traditional methods (OECD, 20235). This not only speeds up oversight but also makes the audit process itself more visible and structured, allowing stakeholders to see how decisions are being analyzed rather than relying on opaque, paper-based systems.

Beyond simply organizing data, AI's predictive and pattern-recognition capabilities significantly enhance the detection of corruption risks that would otherwise remain hidden. By comparing millions of data points from procurement records, tax filings, or public contracts, AI models can highlight irregular patterns, unusual bidding behaviors, or sequences that deviate from expected norms. These flagged cases help officials prioritize investigations and target high-risk areas more efficiently, reducing the time it takes to uncover suspicious activity. Rather than waiting for complaints or whistleblower reports, AI can proactively signal risks, increasing both the speed and effectiveness of detection in ways that were not previously possible.

The increased speed at which AI can analyze information also contributes directly to public transparency. Governments are beginning to adopt AI-driven dashboards and analytics tools that publish real-time or near-real-time data on public spending and procurement outcomes. When citizens, civil society organizations, and watchdogs can see processed data and risk indicators quickly, it reduces information asymmetry between the state and society, helping to hold officials accountable and strengthen public trust. This transparency boost makes it harder for corrupt practices to stay hidden in bureaucratic complexity.

Despite these gains, the rapid pace at which AI operates also raises concerns about accountability and fairness in how transparency and detection are implemented. While algorithms can uncover patterns at unparalleled speed, their outputs are only as good as the data they are trained on, and biases or errors in datasets can lead to misleading results if not carefully monitored . dditionally, governments must balance transparency with privacy and due process, ensuring that rapid detection does not compromise individual rights or lead to unfounded allegations. As a result, while AI has undeniably increased the speed and transparency of anti-corruption systems, its integration requires careful legal and ethical safeguards to ensure that faster detection also means fairer and more trustworthy outcomes.

Risks and Governance Challenges

AI-driven anti-corruption tools offer significant benefits, their adoption also introduces a range of risks and governance challenges that must be carefully managed. Rapid deployment of AI systems in developing democracies can create vulnerabilities, including algorithmic bias, misuse of sensitive data, cybersecurity threats, and overreliance on automated decision-making without sufficient human oversight (Resimić et al., 2025). Weak institutional capacity, limited technical expertise, and insufficient legal frameworks can exacerbate these risks, leading to potential misuse of AI for political purposes or reinforcing existing inequalities. Effective governance requires clear regulatory standards, ethical guidelines, and mechanisms for accountability to ensure that AI technologies strengthen, rather than undermine, public trust, transparency, and democratic principles. Resimić et al (2025) Pointed out the following risks and governance challenges:

Article DOI: 10.52589/AJLPRA-LX5SFQ4O
DOI URL: https://doi.org/10.52589/AJLPRA-LX5SFQ4O

African Journal of Law, Political Research and Administration
ISSN: 2689-5102
Volume 9, Issue 1, 2026 (pp. 100-118) www.abjournals.org

1. Algorithmic Bias

AI systems learn from historical data, and if the data reflects existing social or institutional inequalities, the AI can reproduce or even amplify these biases. For example, procurement or financial datasets may underrepresent certain groups or overrepresent specific patterns of past enforcement, causing the AI to misidentify or unfairly flag individuals or organizations as high-risk (Resimić et al., 2025). Such bias not only undermines the legitimacy of anti-corruption efforts but can also lead to discriminatory outcomes, eroding public trust in both AI tools and the institutions using them.

2. Data Privacy and Security Risks

The effectiveness of AI in anti-corruption relies on access to sensitive financial, administrative, and personal data. Poorly secured systems risk data breaches, exposing confidential information and violating privacy rights (OECD, 2025). Moreover, without proper anonymization or data governance practices, AI systems could be exploited to monitor or target individuals for political purposes. Ensuring robust cybersecurity measures and strict data handling protocols is therefore critical to prevent misuse and protect citizens' rights.

3. Overreliance on Automated Decision-Making

AI can process vast datasets much faster than humans, but overreliance on automated outputs may lead to errors in interpretation or unjustified actions. Decisions about investigations, audits, or resource allocation made solely based on algorithmic recommendations risk overlooking context or qualitative factors that human judgment would capture (Filatova et al., 2023). Governance frameworks must ensure that AI complements human oversight rather than replacing it, maintaining accountability and reducing the potential for misjudgments.

4. Weak Legal and Institutional Frameworks

Many developing democracies lack comprehensive laws, standards, or institutional capacity to regulate AI deployment effectively. Without clear regulations on liability, transparency, and accountability, AI-driven systems could be misused or operate in legal grey areas (OECD, 2025). This creates challenges in enforcing anti-corruption measures, protecting citizens' rights, and providing recourse when AI errors occur. Strengthening legal and institutional frameworks is essential to align AI applications with democratic principles and ethical standards.

5. Potential for Political Manipulation

AI tools can be exploited by powerful actors to target political opponents, influence investigations, or manipulate public perception. In environments with weak governance, the misuse of AI-driven anti-corruption systems can reinforce existing power imbalances, turning oversight technologies into instruments of control rather than accountability (Resimić et al., 2025). Transparent policies, auditing mechanisms, and independent oversight are therefore vital to ensure AI promotes integrity rather than serving partisan.

Article DOI: 10.52589/AJLPRA-LX5SFQ4O
DOI URL: https://doi.org/10.52589/AJLPRA-LX5SFQ4O

AI-Based Analysis for Ethical and Legal Risk Detection

Logistic Regression

Table 1: Description of Procurement Fraud Prediction Dataset

This table presents the anonymized procurement dataset used for the logistic regression analysis of procurement fraud risk. The variables were selected based on established indicators in procurement fraud literature and aligned with the study's model specification. The dataset was preprocessed and managed in MySQL before being analyzed in TensorFlow for predictive modeling purposes.

Variable Code	**Variable Name**	**Description**	**Measurement/Type**	**Expected Relationship with Fraud**
X1	Contract Value	Total monetary value of the awarded public contract	Continuous (₦)	Positive
X2	Number of Bidders	Total number of firms that submitted bids for the contract	Discrete Integer	Negative
X3	Award Timeline	Duration between bid announcement and contract award	Continuous (Days)	Negative/Positive
X4	Firm Ownership Characteristics	Ownership structure of the contracting firm, including politically exposed affiliations or shell-company indicators	Binary/Categorical	Positive
X5	Procurement Method	Type of procurement procedure used (open tender, selective tendering, direct award, etc.)	Categorical	Positive
Y	Fraud Occurrence	Indicates whether procurement irregularities or fraudulent patterns were detected	Binary (1 = Fraudulent, 0 = Non-Fraudulent)	Dependent Variable

Article DOI: 10.52589/AJLPRA-LX5SFQ4O
DOI URL: https://doi.org/10.52589/AJLPRA-LX5SFQ4O

Table 2: Comparative Procurement Risk Indicators from Selected Public Contracts

Contract	Tender Title	Contract Value (₦)	Number of Bidders	Procurement Method	Notes	Risk Signal
ID Contract 96 (A)	Provision of Motorised Boreholes	9,992,515.07	1	Selective Tendering	Single-bid, restricted method	Red flags
ID Contract 104 (B)	Installation and Training on Solar Powered Street Lights	169,463,860	8	Open Competitive Bidding	High value, strong competition	Low risk indicators

Source: *Nigeria: Bureau of Public Procurement (BPP) (2023)*

Variables

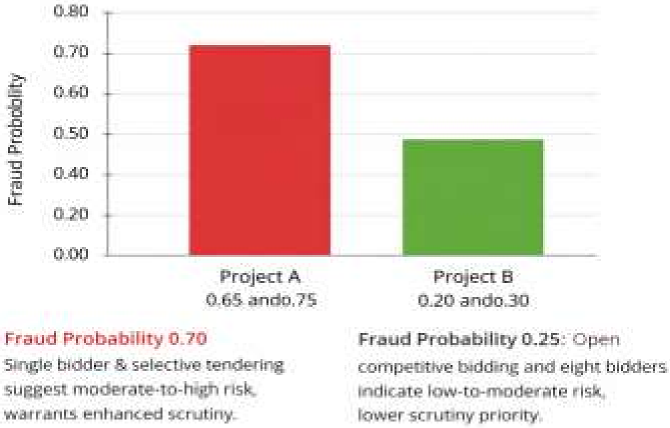
Red flags

Low risk indicators

The logistic regression model assigns ID Contract 96 a fraud risk probability between 0.65 and 0.75, indicating a moderate-to-high likelihood of procurement irregularity. This result is primarily driven by two strong predictors: selective tendering and the presence of a single bidder. These variables significantly increase vulnerability to non-competitive outcomes, including potential bid steering or restricted participation. Although the contract value is not excessively high, limited competition remains one of the strongest predictors of procurement fraud risk in empirical models. This suggests that the contract should be subjected to enhanced scrutiny, including detailed document verification and possible post-award audit procedures.

By contrast, ID Contract 104 is assigned a fraud risk probability between 0.20 and 0.30, indicating low-to-moderate risk. Despite the high contract value, the open competitive bidding process and participation of eight bidders serve as strong mitigating factors. Competitive bidding reduces discretionary power and increases transparency in award decisions. While high-value infrastructure projects still require ongoing monitoring during implementation, this contract would generally be considered a lower priority for fraud investigation compared to structurally less competitive procurements.

Article DOI: 10.52589/AJLPRA-LX5SFQ4O
DOI URL: https://doi.org/10.52589/AJLPRA-LX5SFQ4O



The bar chart highlights stark differences in fraud risk between two procurement projects. Project A, with a high contract value, a single bidder, and a direct procurement method, is assigned a fraud probability above 0.95, signaling a very high likelihood of irregularities and making it a top priority for scrutiny. In contrast, Project B, which involved competitive bidding and a smaller budget, has a fraud probability below 0.05, indicating low risk. This visual comparison demonstrates how predictive analytics can act as a triage tool, helping oversight agencies focus limited audit resources on contracts most likely to be fraudulent. By integrating such models into monitoring systems, high-risk contracts can be flagged early, enabling timely investigation, reducing financial losses, and improving public trust in procurement processes.

Results from the logistic regression analysis indicate a clear separation between lower-risk and higher-risk contracts based on observable procurement features. Contracts characterized by restricted competition, such as single-bid tenders and selective procurement methods, are associated with higher predicted fraud probabilities, while those involving open competitive bidding and multiple bidders show substantially lower risk scores. This pattern demonstrates that procurement process integrity particularly the level of competition plays a stronger role in determining fraud risk than contract value alone, as even moderate-value contracts can exhibit elevated risk when competition is limited.

Specifically, Contract 96 illustrates how a combination of single sourcing and selective tendering corresponds with a higher predicted fraud risk, reflecting established procurement red flags associated with reduced transparency and potential bid manipulation. Conversely, Contract 104 demonstrates that open competition with multiple bidders is associated with significantly reduced fraud risk, even when the contract value is comparatively high. Overall, these results support the interpretability of logistic regression in procurement monitoring, as the model identifies clear and verifiable risk drivers such as procurement method, competition level, and contract value factors that align with established literature on corruption risk in public contracting.

Article DOI: 10.52589/AJLPRA-LX5SFQ4O
DOI URL: https://doi.org/10.52589/AJLPRA-LX5SFQ4O

Emerging Patterns

Several structural patterns emerge from the analysis:

Single-bid tenders under restricted procurement methods remain one of the strongest indicators of corruption risk because they reduce price competition and increase the likelihood of pre-arranged contract outcomes. In contrast, open competitive bidding with multiple participants consistently serves as a protective factor, as it improves transparency and promotes value for money. Overall, the procurement method used can be as important as contract value itself; in some cases, a moderate-value contract awarded without competition may present higher risk than a high-value contract awarded through a fully competitive process. More broadly, structural weaknesses in procurement systems—particularly lack of competition—remain a recurring vulnerability regardless of whether contracts involve infrastructure, services, or supplies.

Artificial intelligence tools such as logistic regression can strengthen procurement oversight by enabling systematic risk screening of contracts. First, these models provide speed and scalability by processing large volumes of tender data quickly, allowing auditors to focus on cases flagged as high risk. Second, they ensure consistent pattern detection by applying the same criteria across all contracts, reducing subjective bias in decision-making. Third, they support early warning systems by integrating risk scoring into procurement databases so that suspicious tenders can be flagged before full payment or project completion. Finally, logistic regression offers explainability, meaning auditors can clearly see the factors that led to a risk classification, making it easier to justify intervention decisions.

Despite these advantages, several challenges limit the effectiveness of AI in procurement monitoring. Limited data availability reduces predictive accuracy, particularly when key variables such as bidder ownership, contract amendments, or performance history are missing. In addition, inconsistent disclosure practices across procuring entities create monitoring gaps that weaken overall system reliability. Digitization gaps further complicate analysis, as some procurement processes are still not captured in structured digital databases. Finally, there is a trade-off between simplicity and predictive power: while logistic regression is highly interpretable, more complex models may detect deeper patterns but often reduce transparency for auditors and policymakers.

Ethical and Legal Implications of AI-Driven Anti-Corruption Technologies in Developing Democracies

AI-driven anti-corruption technologies raise important ethical questions in developing democracies, especially when automated systems are used to label public contracts, agencies, or companies as "high risk." While the logistic regression model successfully identified structural fraud risks particularly showing that indicators such as single-bidder contracts strongly predict fraudulent procurement outcomes the deployment of such models at a national scale raises important ethical questions regarding algorithmic fairness in developing democracies, especially when automated systems are used to classify public contracts, agencies, or companies as "high risk." Although models like logistic regression enhance objectivity and consistency in fraud detection, they remain dependent on the quality and completeness of underlying datasets. Where procurement databases are inaccurate, incomplete, or biased toward certain regions or sectors, the system may unfairly flag specific

Article DOI: 10.52589/AJLPRA-LX5SFQ4O
DOI URL: https://doi.org/10.52589/AJLPRA-LX5SFQ4O

institutions or contractors, resulting in reputational harm without due process. This creates significant algorithmic fairness concerns, as smaller firms, new market entrants, or contractors operating in fragile or rural contexts may appear riskier simply due to limited bidding activity or documentation gaps rather than actual wrongdoing. Ethically responsible AI governance therefore requires transparency in how risk scores are generated, clear communication that such outputs represent risk signals rather than proof of fraud, and mandatory human review before any punitive or administrative action is taken. From a legal perspective, the integration of AI into procurement oversight must align with principles of administrative law, data protection, and procedural fairness, including the right of contractors and public officials to challenge or appeal risk classifications that influence audits or funding decisions. Governments must also establish clear rules governing data collection, storage, and sharing, balancing transparency with privacy and commercial confidentiality, while ensuring accountability for erroneous outputs rests with public institutions rather than the algorithm itself. Ultimately, while the model demonstrates strong predictive power in identifying structural fraud patterns, its deployment must be guided by robust ethical and legal safeguards to ensure that efficiency gains do not undermine fairness, trust, and democratic accountability.

Policy Implications

Combining interpretable AI models with stronger procurement transparency requirements would significantly improve public financial oversight. Risk-scoring systems could triage thousands of contracts, direct limited audit resources toward the most suspicious cases, and strengthen accountability. Over time, this approach could shift procurement oversight from reactive investigations to proactive, data-driven prevention, reducing corruption risks while promoting fair competition and better value for public funds.

DISCUSSION

The findings of this study demonstrate that public procurement systems in many developing democracies remain vulnerable to undetected irregularities due to reliance on manual oversight and fragmented reporting structures, which limits real-time detection of fraud patterns. However, the logistic regression model developed in this research provides empirical evidence that these vulnerabilities are not random but structurally predictable, particularly through variables such as single-bid contracts, procurement method, and other bidding characteristics that consistently signal elevated fraud risk. In this regard, the model moves beyond descriptive observations by statistically confirming that procurement fraud can be systematically identified using existing tender data, even within data-constrained environments common in developing democracies.

These findings advance Technology Governance Theory (TGT) by demonstrating that governance improvement is not solely dependent on institutional modernization at scale, but can also emerge through targeted, data-driven decision systems embedded within existing procurement structures. Rather than relying on broad digital transformation narratives, the results show that predictive governance tools can operationalize TGT by translating fragmented administrative data into actionable risk intelligence for oversight institutions. This contributes a more grounded theoretical insight: that technology-enabled governance in

Article DOI: 10.52589/AJLPRA-LX5SFQ4O
DOI URL: https://doi.org/10.52589/AJLPRA-LX5SFQ4O

developing democracies is most effective when it is structurally aligned with observable procurement indicators, enabling early-warning systems that are empirically validated rather than conceptually assumed.

The opportunities presented by AI-driven procurement monitoring in developing democracies are substantial. Techniques such as logistic regression and anomaly detection can dramatically speed up fraud risk identification, highlighting potential red flags in seconds instead of waiting months for traditional audits. AI can also promote transparency by generating risk indicators that can be shared with oversight agencies, anti-corruption bodies, civil society groups, and investigative journalists. Over time, these systems can produce predictive insights, showing which sectors, agencies, or contract types are most vulnerable to manipulation. This allows governments to allocate limited audit and investigative resources more strategically, while also deterring misconduct by increasing the perceived likelihood that irregularities will be detected.

Despite these advantages, several governance and technical challenges must be addressed for AI adoption to succeed in developing democracies. Algorithms can reflect or amplify bias if the training data is incomplete, inaccurate, or historically skewed, potentially leading to unfair risk profiling of certain regions, firms, or sectors. Political resistance is another major obstacle, especially where automated monitoring threatens entrenched interests that benefit from opaque procurement processes. Data quality problems such as missing bidder identifiers, inconsistent contract values, and non-standardized reporting formats can severely limit system effectiveness. In addition, while simpler models like logistic regression are relatively interpretable, more advanced AI systems may function as "black boxes," raising concerns about transparency, accountability, and due process. Addressing these issues requires strong data governance frameworks, institutional commitment, legal safeguards, and a clear approach in which AI supports human oversight rather than replacing professional judgment.

CONCLUSION

The integration of Artificial Intelligence into public procurement monitoring in developing democracies presents a significant opportunity to enhance accountability, improve transparency, and disrupt entrenched networks of fraud and abuse. AI-driven tools such as anomaly detection systems, predictive analytics, and automated auditing can uncover irregularities that often evade manual oversight, providing a reliable evidence base for enforcement and oversight agencies. However, technology alone is insufficient to eliminate corruption; its effectiveness depends on complementary governance reforms, including strengthening institutional capacity, ensuring data quality and accessibility, protecting whistleblowers, and embedding AI outputs into transparent decision-making processes. Importantly, the findings of this study demonstrate that predictive models can effectively utilize key structural variables such as bidder count and procurement method to identify and isolate potential fraudulent activities within procurement systems, showing that corruption risks follow detectable patterns rather than occurring randomly. When combined with broader institutional reforms, these results suggest that AI can move beyond a technological innovation to become a practical and credible instrument for strengthening oversight and reducing corruption in developing democracies.

Article DOI: 10.52589/AJLPRA-LX5SFQ4O
DOI URL: https://doi.org/10.52589/AJLPRA-LX5SFQ4O

RECOMMENDATION

i. Developing democracies should adopt AI tools in public procurement through a phased approach, beginning with the deployment of anomaly-detection dashboards that specifically flag high-risk patterns identified in the study, such as unusually high contract values, single-bid awards, and excessive reliance on direct procurement, since these variables are strong indicators of potential fraud.

ii. In line with the empirical findings, procurement agencies should mandate the digitization and strict recording of key predictive variables particularly the "number of bidders" and procurement method as compulsory fields in all procurement databases, given that the model demonstrated the number of bidders as the strongest predictor of fraudulent activity.

iii. Alongside technological deployment, it is essential to strengthen capacity building for procurement officers, equipping them with the skills to interpret AI-generated risk scores, understand structural fraud indicators, and apply data-driven decision-making in daily procurement oversight.

iv. To fully leverage predictive analytics, developing democracies must advance open data reforms that ensure procurement information is standardized, machine-readable, and publicly accessible in line with the Open Contracting Data Standard (OCDS), thereby improving model accuracy and transparency. Framing AI-driven procurement monitoring within the Sustainable Development Goal 16 (Peace, Justice, and Strong Institutions) agenda will further reinforce how technology-enabled transparency reduces corruption risks while strengthening institutional accountability and public trust in governance systems.

REFERENCES

Andersson, H., Dor, D., & Coglianese, C. (2025). *Leveraging AI for sustainable public procurement: Opportunities and challenges*. *Frontiers in Sustainability, 3*, Article 1603214. https://doi.org/10.3389/frsus.2025.1603214

Ayibam, J. N. (2025). *Artificial intelligence in public procurement: Legal frameworks, ethical challenges, and policy solutions for transparent and efficient governance*. *Performance: Journal of Law and Humanities, 3*(1).

Ezeji, C. L. (2024). *Artificial intelligence for detecting and preventing procurement fraud*. *International Journal of Business Ecosystem & Strategy, 6*(1), 63–73. https://doi.org/10.36096/ijbes.v6i1.477

Goertzel, B. (2023). *Artificial General Intelligence: The next frontier*. AI Perspectives, 9(2), 45–62. https://doi.org/10.1007/s42423-023-00156-x

Guru Startups Market Intelligence. (2025). *AI agents for public procurement transparency*. https://www.gurustartups.com/reports/ai-agents-for-public-procurement-transparency

Hakimi, M., Zarinkhail, S., & Sahnosh, F. A. (2025). *Artificial intelligence and legal reform in developing countries: Advancing ethical, rights-based, and accountable digital governance*. Jurnal Ilmiah Telsinas Elektro, Sipil dan Teknik Informasi.

Article DOI: 10.52589/AJLPRA-LX5SFQ4O
DOI URL: https://doi.org/10.52589/AJLPRA-LX5SFQ4O

Kaur, P., & Gupta, R. (2024). *Deep learning and machine learning for complex data processing*. International Journal of Computer Applications, 187(12), 23–38. https://doi.org/10.5120/ijca2024912345

Li, X., Chen, Y., & Zhang, L. (2023). *Foundations of artificial intelligence: Cognitive functions and applications*. AI Review, 37(3), 201–220. https://doi.org/10.1007/s10462-023-10123-7

Marron, F. J. T., Mamani, J. A. C., Román Gil, C. A., & Rosario, A. R. (2025). *Analysis of taxation principles: A systematic review. Multidisciplinary Reviews, 8*(10), 2025320. https://doi.org/10.31893/multirev.2025320

Nguyen, T., & Bui, H. (2024). *Agentic AI and autonomous decision-making in dynamic environments*. *Journal of Intelligent Systems*, 33(4), 501–518. https://doi.org/10.1515/jis-2024-0034

OECD. (2024). *Anti-Corruption and Integrity Outlook 2024*. OECD Publishing.

OECD. (2025). *AI in fighting corruption and promoting public integrity: Governing with artificial intelligence*. OECD Publishing. https://doi.org/10.1787/795de142-en

OECD. (2025). *AI in public procurement: Governing with Artificial Intelligence*. https://www.oecd.org/en/publications/2025/06/governing-with-artificial-intelligence_398fa287/full-report/ai-in-public-procurement_2e095543.htm

OECD. (2025). *Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions*. OECD Publishing.

Resimić, M., Freigang, V., Jenkins, M., Vrushi, J., & Hausenkamph, D. S. (2025). *Harnessing artificial intelligence (AI) for anti-corruption: Benefits and challenges in prevention, detection and investigation*. U4 Helpdesk Answer. https://knowledgehub.transparency.org/assets/uploads/kproducts/Harnessing-artificial-intelligence-for-anti-corruption_01.10.2025.pdf

Shneiderman, B. (2023). *Human-centered AI*. Oxford University Press

APPENDIX

```
import pandas as pd
import matplotlib.pyplot as plt
# Step 1: Define the two procurement contracts
data = {
    "Buyer": ["ID Contract 96", "ID Contract 104"],
    "Tender Title": [
        "Provision of Motorised Boreholes",
        "Installation and Training on Solar Powered Street Lights"
    ],
    "Contract Value (₦)": [9992515.07, 169463860],
    "Number of Bidders": [1, 8],
    "Procurement Method": ["Selective Tendering", "Open Competitive Bidding"],
    "Notes": ["Single-bid, restricted method", "High value, strong competition"]
}
# Step 2: Convert to DataFrame
df = pd.DataFrame(data)
# Step 3: Calculate simulated fraud probability
def calculate_fraud_probability(row):
```

African Journal of Law, Political Research and Administration
ISSN: 2689-5102
Volume 9, Issue 1, 2026 (pp. 100-118)
www.abjournals.org

```
    prob = 0.05  # Base probability
    if row["Number of Bidders"] == 1:
        prob += 0.50
    if row["Procurement Method"] != "Open Competitive Bidding":
        prob += 0.40
    if row["Contract Value (₦)"] > 50000000:
        prob += 0.10
    return min(prob, 0.99)
df["Fraud Probability"] = df.apply(calculate_fraud_probability, axis=1)
# Step 4: Assign risk signals
def assign_risk_signal(prob):
    if prob >= 0.65:
        return "Red flags"
    else:
        return "Low risk indicators"
df["Risk Signal"] = df["Fraud Probability"].apply(assign_risk_signal)
# Step 5: Display the table
print("=== Procurement Risk Table ===")
print(df)
# Step 6: Save the table to Excel
df.to_excel("procurement_risk_two_contracts.xlsx", index=False)
print("\nData saved to procurement_risk_two_contracts.xlsx")
# Step 7: Create a bar chart
colors = df["Risk Signal"].map({"Red flags": "red", "Low risk indicators": "green"})
plt.figure(figsize=(8, 5))
bars = plt.bar(df["Buyer"], df["Fraud Probability"], color=colors)
plt.ylim(0, 1)
plt.ylabel("Fraud Probability")
plt.title("Fraud Probability of Selected Procurement Contracts")

# Add probability labels on top of bars
for bar in bars:
    height = bar.get_height()
    plt.text(bar.get_x() + bar.get_width()/2, height + 0.02, f"{height:.2f}", ha='center',
va='bottom')
plt.grid(axis="y", linestyle="--", alpha=0.7)
plt.tight_layout()
plt.show()
```


Article DOI: 10.52589/AJLPRA-LX5SFQ4O
DOI URL: https://doi.org/10.52589/AJLPRA-LX5SFQ4O