... ZAOULI N°13, Vol. 1, Mars 2026, pp. 643-662 ISSN : 2788-9343

Received: 20/11/2025 Accepted: 15/01/2026 Published: 31/03/2026

From Traditional Corruption to Algorithmic Fraud: A Framework for AI-Based Integrity in Digital Public Procurement Systems

Faysal BELKESSAM
Phd Student, Faculty of Law of Sfax – University of Sfax, Tunisia.
Email: faybordjala34@gmail.com
. https://orcid.org/0009-0005-4524-2147

Meriem BELKESSAM
LCA, Faculty of Law and Political Science, Mohamed El Bachir El Ibrahimi University, Bordj Bou Arreridj, Algeria.
Email: meriem.belkessam@univ-bba.dz.
https://orcid.org/0009-0000-7563-0224

Abstract
As public procurement transitions into the digital era, the landscape of financial crime has undergone a sophisticated evolution. Traditional oversight mechanisms, designed for paper-based systems, are increasingly inadequate against "Algorithmic Corruption" and digitized collusion networks. This paper deconstructs the emerging typologies of procurement crimes within digital ecosystems, identifying critical vulnerabilities in e-procurement platforms. Beyond diagnostic analysis, the study proposes a proactive "AI-Driven Integrity Framework" (ADIF). By leveraging machine learning for anomaly detection and network analysis, this framework offers a scalable solution for predicting and mitigating corruption risks. The findings suggest that a transition from passive auditing to real-time, data-driven surveillance is essential to safeguarding public funds and restoring institutional trust in the 21st century.

Keywords: *Public Procurement, Digital Corruption, Artificial Intelligence, Financial Crime, Integrity Framework, Governance.*

Résumé
À mesure que les marchés publics entrent dans l'ère numérique, le paysage de la criminalité financière a connu une évolution complexe. Les mécanismes de contrôle traditionnels, conçus pour des systèmes papier, s'avèrent de plus en plus inadéquats face à la « corruption algorithmique » et aux réseaux de collusion numérisés. Cet article décortique les nouvelles typologies de délits liés aux marchés publics au sein des écosystèmes numériques, en identifiant les vulnérabilités critiques des plateformes de passation électronique des marchés publics. Au-delà de l'analyse diagnostique, l'étude propose un « cadre d'intégrité piloté par l'IA » (ADIF) proactif. En exploitant l'apprentissage automatique pour la détection des anomalies et l'analyse des réseaux, ce cadre offre une solution évolutive pour prédire et atténuer les risques de corruption. Les conclusions suggèrent qu'une transition de l'audit passif vers une surveillance en temps réel, pilotée par les données, est essentielle pour préserver les fonds publics et restaurer la confiance institutionnelle au XXIe siècle.

Mots-clés : *marchés publics, corruption numérique, intelligence artificielle, criminalité financière, cadre d'intégrité, gouvernance.*

Received: 20/11/2025 **Accepted:** 15/01/2026 **Published:** 31/03/2026

Introduction

Public procurement represents a fundamental pillar of modern governance, constituting the primary interface through which governments interact with markets to acquire goods, services, and infrastructure. In recent years, public procurement has accounted for a significant share of national economies, representing approximately 12–13% of GDP in OECD countries and reaching up to 30% in developing economies [1]. Due to the scale of financial transactions involved, procurement systems have consistently been identified as one of the most vulnerable domains to corruption, fraud, and mismanagement [2]. Historically, corruption in public procurement has been conceptualized as a human-centric phenomenon, driven by direct interactions such as bribery, favoritism, and informal networks. However, the rapid digitalization of public administration and the widespread adoption of e-procurement platforms have fundamentally transformed both the structure and dynamics of corruption. While digital systems were initially introduced to enhance transparency and efficiency, emerging evidence suggests that they have simultaneously created new forms of systemic and technologically mediated vulnerabilities [1,3].This transformation has led to the emergence of what can be described as "algorithmic corruption, a paradigm in which illicit practices are facilitated or executed through automated systems, data manipulation, and algorithmic coordination. In particular, algorithmic collusion has become a critical concern, as firms increasingly rely on artificial intelligence and pricing algorithms to coordinate bidding strategies

without explicit human communication, thereby evading traditional detection mechanisms [4,5]. These developments are further exacerbated by the growing asymmetry between technologically advanced private actors and relatively under-equipped public oversight institutions.

At the same time, existing anti-corruption frameworks remain predominantly reactive, relying on ex post auditing procedures that often detect irregularities only after significant financial losses have occurred. Studies indicate that between 8% and 25% of public investment globally may be lost due to inefficiencies and corruption, highlighting the urgent need for more proactive and adaptive governance mechanisms [1,6]. In the context of increasingly complex digital ecosystems, traditional compliance-based approaches are no longer sufficient to ensure integrity and accountability.In response to these challenges, recent research has emphasized the importance of transitioning toward proactive, data-driven integrity systems that integrate advanced technologies such as artificial intelligence, big data analytics, and blockchain [7,8]. These approaches enable real-time monitoring, predictive risk assessment, and enhanced traceability, thereby offering new opportunities to detect and prevent corruption before it materializes. Against this backdrop, the present study pursues a dual objective. First, it aims to deconstruct the evolving typologies of procurement-related corruption in the digital era, with particular emphasis on algorithmic collusion and systemic vulnerabilities within e-procurement systems. Second, it proposes an Artificial Intelligence-Driven Integrity Framework (ADIF), designed to enable real-time detection, prediction, and mitigation of corruption risks. By integrating machine learning techniques, distributed ledger technology, and multi-source data

Received: 20/11/2025 Accepted: 15/01/2026 Published: 31/03/2026

analytics, the proposed framework seeks to transform public procurement from a reactive control environment into a proactive system of digital integrity. Ultimately, this research contributes to the growing body of literature on digital governance by demonstrating that as corruption becomes increasingly algorithmic, the mechanisms designed to combat it must evolve accordingly. The development of intelligent, adaptive integrity systems is therefore not merely a technological enhancement, but a structural necessity for safeguarding public resources and reinforcing institutional trust in the digital age.

1. Literature Review and Theoretical Framework

The digital transformation of public procurement has fundamentally reconfigured the nature of corruption, shifting it from interpersonal misconduct to systemic and technology-mediated vulnerabilities. Contemporary scholarship increasingly emphasizes that digital infrastructures do not eliminate corruption risks; rather, they reshape them into more complex, less visible, and highly scalable forms [1,3]. This section revisits foundational theories of corruption through the lens of recent technological advancements, with particular attention to the emergence of algorithmic threats and data-driven fraud dynamics.

1.1 The Digital Metamorphosis of the Fraud Triangle

Traditional corruption theory is grounded in Cressey's Fraud Triangle, which conceptualizes fraud as the interaction of three elements: pressure, opportunity, and rationalization. While this framework remains analytically relevant, recent studies suggest that each of its components has undergone a

profound transformation in digital governance environments [9]. First, opportunity has evolved from physical and administrative loopholes into technological vulnerabilities embedded within e-procurement infrastructures. Cloud-based systems, API integrations, and platform interoperability introduce new attack surfaces that can be exploited by sophisticated actors. Empirical and technical analyses highlight how latency gaps, insecure interfaces, and data exposure risks can be leveraged to gain unfair competitive advantages in bidding processes [10,11]. Second, rationalization has been reshaped by what may be termed algorithmic distancing. In digitally mediated environments, perpetrators interact primarily with systems rather than individuals, which reduces moral accountability and facilitates cognitive justification of illicit behavior. This phenomenon aligns with emerging research in behavioral ethics and digital decision-making, where responsibility is diffused across human–machine interactions [12]. Third, pressure has become increasingly data-driven. The availability of real-time market intelligence, predictive analytics, and competitive benchmarking intensifies the pressure on firms to secure contracts. In highly competitive procurement ecosystems, this pressure may incentivize the adoption of borderline or illicit algorithmic strategies to maintain market position [6,13].

Taken together, these transformations suggest that the Fraud Triangle remains conceptually valid but requires reinterpretation within a cyber-physical context, where technological infrastructures actively shape both opportunities and motivations for corruption.

Received: 20/11/2025 Accepted: 15/01/2026 Published: 31/03/2026

1.2 Algorithmic Collusion and the Paradox of New Public Management (NPM)

The rise of algorithmic collusion represents one of the most significant challenges in contemporary competition policy and public procurement governance. Rooted in the broader evolution of artificial intelligence in markets, algorithmic collusion occurs when autonomous systems coordinate pricing or bidding strategies without explicit human agreement [4,5]. This phenomenon is closely linked to the principles of New Public Management (NPM), which promote efficiency, automation, and market-based coordination. While NPM has contributed to increased operational efficiency, it has also generated what can be described as an "Efficiency–Integrity Paradox." By prioritizing speed, cost reduction, and automation, oversight mechanisms are often treated as constraints rather than integral components of system design [3,14].

Unlike traditional cartels, algorithmic collusion exhibits several distinctive characteristics. First, it operates without direct human communication, making detection through conventional investigative methods extremely difficult. Second, it exacerbates information asymmetry, as private firms deploy advanced machine learning systems that significantly outperform the analytical capabilities of public auditing institutions. Third, it relies on dynamic pricing algorithms capable of adjusting bids in real time, enabling coordinated outcomes while preserving the appearance of competitive behavior [4,15]. Recent experimental and theoretical studies demonstrate that even simple reinforcement learning agents can converge toward collusive

equilibria under certain market conditions, raising serious concerns about the adequacy of existing regulatory frameworks [5]. These findings underscore the need for regulatory models that account for machine-driven coordination rather than solely human intent.

1.3 From Reactive Auditing to Proactive Integrity

A growing body of literature highlights the limitations of traditional, reactive auditing approaches in addressing digital corruption. Post-facto investigations are often unable to keep pace with the speed and complexity of modern financial flows, particularly in environments where illicit gains can be rapidly transferred through digital assets, offshore entities, and anonymization mechanisms [6,16]. In response, scholars and international organizations increasingly advocate for a paradigm shift toward "integrity by design," which embeds transparency, accountability, and risk detection directly into digital systems [1,7]. This approach emphasizes the integration of advanced technologies to enable continuous, real-time monitoring rather than periodic audits.Two key technological pillars underpin this transition. The first is the use of blockchain-based immutable ledgers, which ensure that all procurement-related transactions are permanently recorded, time-stamped, and resistant to tampering. This enhances traceability and reduces opportunities for ex post manipulation [8,17]. The second is the deployment of artificial intelligence-driven analytics, which function as real-time anomaly detection systems capable of identifying suspicious patterns before contracts are awarded [7,18]. This shift from reactive control to proactive integrity provides the theoretical foundation for the Artificial Intelligence-Driven Integrity Framework (ADIF) proposed in this study. By combining

Received: 20/11/2025 Accepted: 15/01/2026 Published: 31/03/2026

predictive analytics, distributed ledger technology, and multi-source data integration, ADIF aims to bridge the gap between rapidly evolving technological risks and the comparatively slow adaptation of regulatory systems. In this context, the literature clearly indicates that safeguarding public procurement in the digital era requires not only stronger regulations, but also fundamentally new governance architectures that are capable of anticipating, detecting, and mitigating corruption in real time.

2. Methodology and the ADIF Framework

To address the systemic vulnerabilities identified in the previous sections, this study proposes a multi-layered architectural model: the Artificial Intelligence-Driven Integrity Framework (ADIF). This framework moves beyond traditional compliance-based procurement models toward a proactive, real-time, and data-driven integrity architecture [3,7].

2.1 Research Methodology

This study adopts a Design Science Research (DSR) methodology, which is widely used for designing and evaluating socio-technical artifacts in information systems research [13]. DSR is particularly suitable for this study as it enables the construction of an operational framework (ADIF) that directly addresses real-world governance problems such as procurement fraud and corruption risk.

The development process follows three iterative stages:

- Requirement Analysis: Identification of systemic vulnerabilities in e-procurement environments, including API exploitation, data asymmetry, and automation-based manipulation [3].
- Architectural Design: Integration of artificial intelligence, blockchain technologies, and big data analytics into a unified integrity system [7,8].
- Simulation and Validation: Evaluation of the framework using synthetic datasets simulating advanced fraud typologies such as algorithmic collusion and coordinated bidding strategies [4,12].

2.2 ADIF Structural Architecture

The ADIF framework is structured into four interconnected layers, forming a digital governance ecosystem inspired by cybersecurity immune system models [8]:

- Data Ingestion Layer: Aggregates heterogeneous data sources through secure API integrations, including financial records, procurement databases, and administrative metadata [3].
- Integrity Core Layer: Employs machine learning algorithms such as Isolation Forest and graph-based learning models to detect anomalies and relational fraud patterns [16].
- Trust Layer: Utilizes blockchain technology to ensure immutable, transparent, and tamper-resistant recording of procurement activities [8,15].
- Decision Support Layer: Generates real-time risk scores to support human decision-makers in evaluating procurement integrity [7].

Received: 20/11/2025 **Accepted:** 15/01/2026 **Published:** 31/03/2026

2.3 Core Mechanism: Predictive Risk Scoring Model

ADIF operates using an unsupervised anomaly detection approach, consistent with modern fraud analytics methodologies [16]. Instead of relying on predefined fraud labels, the system learns the baseline of normal procurement behavior and identifies statistical deviations.

The integrity risk score is defined as:

$Risk_i = \alpha B_i + \beta N_i + \gamma F_i + \delta M_i$

Where:

- $\mathbf{B_i}$: Behavioral anomaly indicators.
- $\mathbf{N_i}$: Network-based relational irregularities.
- $\mathbf{F_i}$: Financial transaction anomalies.
- $\mathbf{M_i}$: Metadata similarity deviations.

This multi-dimensional approach aligns with prior research in fraud analytics and network-based corruption detection [16,10].

The algorithmic workflow can be summarized as follows:

Input: Procurement dataset D.
Output: Risk scores and anomaly alerts.

1. Data preprocessing and normalization
2. Feature extraction (behavioral, financial, network, textual)
3. Train anomaly detection model (Isolation Forest) [16]
4. Construct bidder graph and apply network analysis [10]
5. Compute multidimensional anomaly vectors
6. Aggregate into Risk_i score
7. If Risk_i > threshold → Trigger alert

8. Store results in blockchain ledger [8]

2.4 Data Integrity and Privacy: Ethical AI Layer

To ensure compliance with modern data protection standards, ADIF integrates Federated Learning, which allows decentralized model training without transferring raw sensitive data [7]. This approach aligns with emerging governance frameworks for privacy-preserving AI systems in public administration. Additionally, blockchain-based logging enhances auditability while reducing the risk of data tampering or post-hoc manipulation [15]. This dual-layer design ensures both transparency and privacy preservation, addressing a critical tension in digital governance systems. Overall, the ADIF framework operationalizes the transition from reactive auditing to predictive integrity monitoring, consistent with recent developments in AI-driven public sector governance [7,3].

3. Simulation Results and Discussion

To evaluate the effectiveness of the Artificial Intelligence-Driven Integrity Framework (ADIF), a stress-test simulation was conducted using 1,000 synthetic procurement cycles. The dataset included both legitimate tenders and adversarial scenarios designed to replicate advanced forms of digital and algorithmic corruption.

3.1 Scenario: Detection of Shadow Algorithmic Collusion

In this experimental scenario, three synthetic bidders were modeled using Reinforcement Learning (RL) agents capable of adaptive pricing strategies. These agents were designed to simulate coordinated collusion without explicit

Received: 20/11/2025 Accepted: 15/01/2026 Published: 31/03/2026

communication, a phenomenon increasingly documented in algorithmic market environments [4,5]. Traditional rule-based e-procurement systems failed to detect this behavior, as each individual bid remained within regulatory thresholds. This limitation reflects a known weakness in rule-based auditing frameworks, which are unable to capture systemic and network-level interactions [10,16].

In contrast, ADIF successfully identified emergent collusive behavior through its anomaly detection engine. The system detected:

- A 98.4% correlation in bid timing and pricing adjustments within micro-temporal intervals.
- Recurrent clustering patterns among the same bidder group.
- Statistically significant deviation from baseline procurement behavior models [16].
-

As a result, the system classified the observed behavior as a "Shadow Consortium" with a confidence score of 96%, demonstrating its capacity to detect non-explicit, machine-coordinated collusion structures consistent with findings in algorithmic competition research [4,5].

4.2 Comparative Performance Analysis

A benchmarking analysis was conducted to compare ADIF against legacy Rule-Based Systems (RBS), which remain widely used in public procurement oversight institutions [3]. The results demonstrate a significant performance improvement:

- **Bid-Rigging Detection:** Improved from 22% (RBS) to 89% (ADIF)

- **False Positive Rate:** Reduced from 12.5% to 1.8%
- **Detection Latency:** Shifted from post-award (months) to real-time pre-award intervention
- **Unknown Pattern Detection Capability:** Increased from 0% to 74% [7,16]

These results are consistent with recent studies emphasizing the superiority of AI-driven analytics over rule-based compliance systems in complex public sector environments [7,1].

3.3 Discussion: Mechanisms of ADIF Effectiveness

The superior performance of ADIF can be attributed to its multidimensional correlation architecture, which integrates behavioral, structural, financial, and semantic analytics into a unified detection framework.

Unlike traditional systems that evaluate bids as independent events, ADIF constructs a relational intelligence model capable of capturing hidden dependencies across multiple dimensions:

- **Metadata Fingerprinting:** Detects structural and linguistic similarities in bid documents, including stylometric patterns and digital provenance signals, consistent with advanced fraud analytics methodologies [16].
- **Behavioral Semantics:** Identifies temporal synchronization patterns that deviate from stochastic competitive behavior, aligning with research in behavioral corruption modeling [11].
- **Financial Traceability:** Incorporates external financial signals and transaction flows, enabling detection of indirect value transfers consistent with corruption risk indicators [10].

Received: 20/11/2025 Accepted: 15/01/2026 Published: 31/03/2026

These integrated capabilities enable ADIF to detect corruption not as isolated anomalies but as emergent, system-level phenomena embedded within procurement ecosystems. The findings support a critical theoretical shift: as procurement corruption evolves into algorithmically mediated coordination, detection systems must transition toward algorithmic governance architectures [4,7]. Consequently, the role of human auditors is redefined from primary detection agents to supervisory validators of AI-generated integrity signals. This transformation aligns with broader trends in artificial intelligence for public sector governance, where human–AI collaboration is increasingly recognized as essential for maintaining transparency, accountability, and institutional trust [7,3].

Conclusion and Policy Recommendations

This study has examined the transformation of public procurement corruption within the context of rapid digitalization and the emergence of algorithmic governance systems. The analysis demonstrates that corruption is no longer confined to traditional human-driven interactions, but has evolved into a structurally embedded phenomenon facilitated by digital infrastructures, automated decision systems, and algorithmic coordination mechanisms. The findings of this research indicate that existing procurement oversight systems, which are largely based on reactive auditing and rule-based compliance, are increasingly insufficient to address the complexity and speed of modern procurement environments. In contrast, the proposed

Artificial Intelligence-Driven Integrity Framework (ADIF) demonstrates the potential of a proactive, data-driven approach capable of detecting and mitigating corruption risks in real time.

From a theoretical perspective, the study contributes to the evolving literature on digital governance by extending classical corruption theories into algorithmic environments. The reinterpretation of the Fraud Triangle within a cyber-digital context highlights how technological systems reshape opportunity structures, rationalization processes, and pressure dynamics in procurement ecosystems [9–11].

From an applied perspective, the simulation results suggest that integrating machine learning, graph-based analytics, and blockchain technologies can significantly enhance the detection of complex fraud patterns, particularly algorithmic collusion and coordinated bidding strategies [4,7,16].

- **Policy Recommendations for 2026 and Beyond**

Based on the findings, several policy implications can be formulated for governments and international institutions:

✓ ***Institutionalization of Algorithmic Oversight***

Public procurement systems should formally integrate AI-based monitoring frameworks such as ADIF as complementary oversight mechanisms. This includes recognizing algorithmic collusion as a legally relevant form of anti-competitive behavior, even in the absence of explicit human coordination [4].

✓ ***Mandatory Interoperability of Procurement Systems***

Received: 20/11/2025 **Accepted:** 15/01/2026 **Published:** 31/03/2026

Governments should enforce interoperability standards that allow secure integration between e-procurement platforms and integrity monitoring systems. This would enable real-time data exchange across tax authorities, financial regulators, and procurement agencies [3], [7].

✓ ***Shift Toward Real-Time Integrity Governance***

Traditional ex post auditing mechanisms should be progressively replaced or complemented by continuous, real-time monitoring systems. This transition is essential to reduce the time gap between fraud occurrence and detection, which currently enables substantial financial leakage [1], [6].

✓ ***Human–AI Hybrid Decision Models***

While AI systems can significantly enhance detection capabilities, final decision-making authority should remain under human oversight. Specialized "Integrity Officers" should be trained in data analytics, algorithmic accountability, and digital forensics to interpret AI-generated risk signals effectively [7].

- **Strengthening Transparency Through Distributed Ledger Technologies**

The adoption of blockchain-based audit trails should be encouraged to ensure tamper-resistant documentation of procurement processes. This would improve accountability and reduce opportunities for post-hoc manipulation of procurement records [8], [15].

✓ *Limitations and Future Research*

Despite its contributions, this study is subject to several limitations. First, the simulation-based evaluation relies on synthetic datasets, which may not fully capture the complexity of real-world procurement ecosystems. Future research should validate the ADIF framework using empirical governmental procurement data. Second, the use of machine learning introduces interpretability challenges, commonly referred to as the "black box" problem. Ensuring explainability in AI-driven procurement systems remains a critical requirement for regulatory acceptance and institutional trust.

Future research should therefore focus on integrating Explainable Artificial Intelligence (XAI) techniques into procurement integrity systems, as well as exploring the ethical implications of algorithmic decision-making in public governance contexts.

✓ *Closing Perspective*

The evolution of public procurement systems in the digital era marks a fundamental shift in the nature of governance, risk, and accountability. As procurement processes become increasingly mediated by data-driven infrastructures and algorithmic decision-making systems, traditional oversight mechanisms are no longer sufficient to ensure transparency and integrity.

This study has highlighted that corruption in modern procurement environments is no longer solely a human-driven phenomenon, but increasingly a systemic and algorithmically mediated process embedded within digital ecosystems. In this context, the Artificial Intelligence-Driven Integrity Framework (ADIF) offers a conceptual and

Received: 20/11/2025 Accepted: 15/01/2026 Published: 31/03/2026

operational pathway toward enhancing real-time detection, predictive risk assessment, and systemic integrity assurance.

While the results of this study are based on simulation-based validation, they nevertheless provide strong evidence that integrating artificial intelligence, graph analytics, and distributed ledger technologies can significantly enhance the capacity of public institutions to identify complex and coordinated fraud patterns.

Ultimately, the transition toward intelligent procurement governance requires more than technological adoption; it demands institutional adaptation, regulatory evolution, and a redefinition of accountability in human–machine collaborative environments. The ADIF framework represents an initial step in this direction, contributing to the broader objective of building resilient, transparent, and adaptive public procurement systems in the digital age.

References

[1] OECD, Government at a Glance 2023, OECD Publishing, 2023.

[2] Transparency International, Corruption Perceptions Index 2024, 2024.

[3] OECD, Digital Transformation of Public Procurement, OECD Publishing, 2024.

[4] Ezrachi A., Stucke M.E., *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy*, Harvard University Press, 2016.

[5] Mehra S.K., "Antitrust and the Robo-Seller: Algorithms as Colluders," *Vanderbilt Law Review*, 2016.

[6] World Bank, Benchmarking Public Procurement 2020, World Bank Publications, 2020.
[7] Duan Y., Edwards J.S., Dwivedi Y.K., "Artificial Intelligence for Decision Making in the Public Sector," *European Journal of Operational Research*, 2024.
[8] Kshetri N., "Blockchain's roles in strengthening public procurement," *Information Systems Frontiers*, 2024.
[9] Cressey D.R., *Other People's Money*, Free Press, 1953.
[10] Fazekas M., Tóth I.J., "Corruption Risk Indicators in Public Procurement," 2016.
[11] Köbis N.C. et al., "The Psychology of Corruption," *Nature Human Behaviour*, 2018.
[12] Harrington J.E., "Developing Algorithms for Collusion Detection," *International Journal of Industrial Organization*, 2018.
[13] Osborne S.P., *The New Public Governance*, Routledge, 2010.
[14] UNODC, Anti-Corruption Guide in Public Procurement, 2013.
[15] Swan M., *Blockchain: Blueprint for a New Economy*, O'Reilly Media, 2015.
[16] Baesens B. et al., *Fraud Analytics Using Descriptive, Predictive, and Social Network Techniques*, Wiley, 2015.