ITJ | The International Tax Journal

# Criminal governance for the protection of public funds in the age of artificial intelligence: A prospective analytical study within the Algerian legal framework

**Dr. Nadjib Beroual** [1] and **Dr. Walid Terki** [2]

[1] University of Batna1, Algeria. Email: nadjib.beroual@univ-batna.dz
[2] Faculty of Law and Political Science, Badji Mokhtar-Annaba University, Algeria. Email: E-mail: walid.terki@univ-annaba.dz

**Abstract---**The management of public funds in Algeria is undergoing profound transformations as a result of the rapid expansion of public administration digitization and the increasing reliance on artificial intelligence technologies in public finance domains, such as public procurement, taxation, and treasury management. While this digital transformation has contributed to enhancing efficiency and promoting transparency, it has simultaneously generated emerging legal risks that threaten the integrity of public funds. This is particularly evident with the rise of new forms of intelligent crimes based on algorithmic manipulation of data, deepfake technologies, and indirect digital embezzlement—practices that often exceed the regulatory and deterrent capacity of traditional criminal law provisions. This study aims to analyze the extent to which the Algerian criminal justice system is capable of establishing effective criminal governance to protect public funds in the face of AI-driven digital risks. It does so by examining the conceptual framework of intelligent crime, analyzing the issue of criminal liability within algorithmic environments, and assessing the effectiveness of the currently adopted preventive and punitive mechanisms. The research adopts an analytical approach in examining relevant national legal texts, alongside a prospective approach to anticipate the future of criminal policy in addressing intelligent crimes. The study concludes that there exists a legislative and institutional gap in dealing with the risks posed by artificial intelligence to public funds, which necessitates a shift from a reactive protection logic toward a preventive criminal governance approach.

**How to Cite**:
Beroual, N., & Terki, W. (2026). Criminal governance for the protection of public funds in the age of artificial intelligence: A prospective analytical study within the Algerian legal framework. *The International Tax Journal*, *53*(1), 436–446. Retrieved from https://internationaltaxjournal.online/index.php/itj/article/view/534

The International tax journal ISSN: 0097-7314 E-ISSN: 3066-2370 © 2026

Submitted: 24 January 2025 | Revised: 09 February 2025 | Accepted: 12 May 2025

**Keywords---**Artificial Intelligence, Criminal Governance, Protection of Public Funds, Digital Crimes, Digital Governance, Algerian Legislation.

## Introduction

1. General Context and Theoretical Background

Over the past decade, the administrative system in Algeria has undergone a profound transformation toward what may be described as comprehensive digital administration. Digital transformation has no longer remained a temporary technical option; rather, it has evolved into a strategic and sovereign-oriented policy aimed at modernizing public services and achieving effective governance of public expenditure. This trajectory has been reinforced through the adoption of the "Digital Algeria" project, which has led to the integration of advanced technologies into the management of sensitive financial sectors, such as electronic public procurement portals, digital taxation systems, and forward-looking financial oversight platforms.

With the introduction of generative artificial intelligence technologies and predictive algorithms into the processing of large-scale public treasury data, new opportunities have emerged to rationalize public spending and enhance transparency and efficiency in financial decision-making. However, this transition toward what is commonly referred to as "administrative intelligence" has not been without challenges. It has simultaneously given rise to novel criminal risks of a non-traditional nature. New forms of financial crime have emerged, characterized by sophistication and complexity, in which algorithms are employed to carry out complex cyber embezzlement schemes, manipulate public procurement criteria through automated processes, or even forge the digital identities of financial officials using deepfake technologies. Such practices expose public funds to risks that exceed the regulatory and enforcement capacity of traditional legal mechanisms.

2. Research Problem

In light of these transformations, the central research problem of this study revolves around the following question:

*To what extent is the Algerian criminal justice system, through its substantive and procedural mechanisms, capable of achieving effective criminal governance for the protection of public funds against AI-enhanced cyber threats, given the inadequacy of classical concepts of deterrence and criminalization to encompass algorithmic criminal conduct?*

This question reflects the core tension between the rapid pace of technological innovation, on the one hand, and the capacity of the criminal legal system to adapt to unprecedented forms of criminal behavior, on the other.

3. Research Hypotheses

This study is based on three main hypotheses:

- **First hypothesis:** There exists a clear legislative gap between the rapid development of artificial intelligence systems and the slow responsiveness of the Algerian Penal Code, which may allow certain emerging acts to escape criminalization, in contradiction with the principle of legality in criminal law.
- **Second hypothesis:** Traditional rules of criminal liability, founded on the concepts of free will and the natural perpetrator, face substantial difficulties in identifying the offender in crimes committed through autonomous systems, thereby necessitating a reconsideration of the scope of liability attributed to legal persons and software developers.
- **Third hypothesis:** Addressing these challenges cannot be achieved through subsequent deterrence alone; rather, it requires the establishment of a preventive criminal governance model that leverages artificial intelligence itself for the early detection of corruption before its occurrence.

4. Objectives and Significance of the Study

The significance of this research stems from its engagement with one of the most pressing contemporary issues in Algeria, particularly in the context of accelerated digital transformation. The study seeks to achieve several key objectives, namely:

- **Conceptual grounding:** Developing a theoretical and legal framework for artificial intelligence–related crimes affecting public funds.
- **Legislative assessment:** Identifying shortcomings in Law No. 06-01 on the Prevention and Combating of Corruption, as well as in the Penal Code, in addressing the challenges posed by comprehensive digitization.
- **Prospective construction:** Proposing practical recommendations that would enable the Algerian legislator to adopt a technologically informed criminal policy aligned with contemporary cyber threats.

5. Methodology

This study adopts a critical analytical methodology in examining relevant Algerian legal texts, supported by an analysis of selected international conventions and standards related to artificial intelligence. It also employs a comparative approach by drawing on European experience, particularly the European Union's Artificial Intelligence Act (AI Act), with the aim of identifying best practices in algorithmic governance. In addition, a prospective methodology is used to analyze future threat scenarios that may target public funds within the framework of Algeria's digital administration.

## I. Conceptual and Methodological Framework

### 1.1. Artificial Intelligence and Public Funds: The Conceptual Framework

#### 1.1.1. The Concept of Generative Artificial Intelligence

Generative artificial intelligence constitutes a branch of artificial intelligence that focuses on the design of models capable of producing original content—whether textual, visual, or digital data—based on extensive and diverse training datasets (Straub, Morgan, Bright, & Margetts, 2022). These models rely on deep learning and machine learning algorithms to generate innovative outputs, distinguishing them from traditional analytical models that are limited to pattern recognition and data analysis.

In the administrative context, generative artificial intelligence serves as a tool for enhancing efficiency and informed decision-making within public administration, particularly through the processing of big data, the improvement of public services, and the support of predictive oversight mechanisms (Digital Government Authority, 2025). However, the capacity of such systems to autonomously generate content also introduces new risks, especially when intelligent systems are employed in fraudulent activities or in the manipulation of financial data, thereby exposing public funds to sophisticated cyber threats (Straub et al., 2022).

#### 1.1.2. Public Funds in the Digital Environment

Public funds encompass financial resources owned by the state or derived from its revenues, which are allocated for the implementation of public policies and the realization of the public interest (Wikipedia, 2025a). Within the digital environment, the management of public funds has become intrinsically linked to comprehensive digitization, including electronic procurement systems, digital taxation platforms, and intelligent financial oversight mechanisms.

While the deployment of artificial intelligence in public financial management enables advanced data analysis, anomaly detection, and more efficient monitoring of public expenditure, it simultaneously raises novel legal and criminal challenges. These challenges are particularly pronounced with respect to attributing responsibility for offenses committed by autonomous digital systems (Wikipedia, 2025b).

#### 1.1.3. The Shift from Traditional Crime to Algorithmic Crime

Algorithmic crimes differ fundamentally from traditional crimes in that the actus reus is executed partially or entirely by intelligent algorithms or autonomous computational systems. Such crimes include

cyber-enabled embezzlement, manipulation of financial data, and the falsification of digital identities through deepfake technologies (Kurshan, Mehta, Bruss, & Balch, 2024).
This transformation necessitates a re-examination of classical criminal liability doctrines founded on free will and the natural perpetrator. In the context of algorithmic crime, responsibility must be carefully allocated among the software developer, the system user, and the legal entity, in a manner that reflects the distinctive characteristics of contemporary digital offenses (Kurshan et al., 2024).

1.2. The Digital Criminal Governance Approach
Digital criminal governance represents a new generation of criminal policy frameworks, in which reliance on rigid punitive rules alone is no longer sufficient. Instead, it has become imperative to integrate technology into the core of the legal process in order to create a structurally "crime-resistant" environment (Straub et al., 2022). This approach facilitates a shift from traditional deterrence models toward a proactive framework grounded in digital oversight and intelligent analytics, thereby ensuring comprehensive protection of public funds.

1.2.1. The Concept of Criminal Governance: From Traditional Oversight to Intelligent Risk Management
Criminal governance should not be understood merely as a set of administrative procedures; rather, it constitutes an integrated regulatory and operational framework aimed at formulating a flexible and automated criminal response. It serves as a strategic nexus between legal rigor, institutional oversight mechanisms, and advanced technological solutions designed to safeguard public funds. While its legitimacy is rooted in the principles of good governance, it transcends them through the adoption of algorithmic transparency and digital accountability (Straub & Bright, 2023).
This governance model relies on real-time monitoring systems capable of analyzing massive financial flows, enabling a transition from slow, paper-based oversight to instantaneous digital supervision. Such systems are able to detect suspicious patterns and fraudulent behavior within seconds, thereby significantly reducing opportunities for the misappropriation of public funds before substantial losses occur (OECD, 2024).
Within this context, the concept of Digital Criminal Resilience may be introduced to denote the capacity of public financial administration to rapidly recover from cyberattacks or embezzlement attempts through robust digital governance systems. This resilience, in turn, enhances trust in national financial policies and institutions (United Nations Development Programme, 2022).

1.2.2. The Methodological Shift from Reactive Deterrence to Proactive Prevention
Given the fluid nature of cybercrime and the inherent difficulties associated with tracing misappropriated digital assets, ex post punitive sanctions have proven insufficient. Consequently, a fundamental shift toward proactive prevention—often conceptualized as *Crime Prevention by Design*—has emerged, whereby legal rules are embedded directly into the code of digital systems (Straub et al., 2022).
Proactive prevention relies on predictive artificial intelligence, which goes beyond post-offense detection to perform the following functions:

- **Analysis of procurement and contractual behaviors:** Comparing ongoing transactions against reliable historical patterns to identify anomalies (*Anomaly Detection*) (Kurshan et al., 2024).
- **Prediction of corruption risks:** Employing mathematical models to identify potential vulnerabilities within public procurement systems and digital taxation frameworks, thereby enabling preventive intervention before damage occurs (United Nations Office on Drugs and Crime, n.d.).

This transition results in the establishment of a self-secured criminal system, in which the protection of public funds becomes an automated, technology-driven function. Such a system minimizes human intervention—often susceptible to error or temptation—and transforms criminal policy from a reactive paradigm into a proactive governance model (OECD, 2024).

Moreover, digital criminal governance acquires a strategic dimension as an instrument for strengthening digital sovereignty over national financial data. This ensures Algeria's institutional autonomy in confronting cross-border threats and transnational cybercrime (European Commission, 2023).

## II. The Digital Criminal Governance Approach

### 2.1. The Concept and Philosophy of Digital Criminal Governance

This section constitutes the theoretical framework that links procedural regulation with modern technological instruments.

#### 2.1.1. The Concept of Criminal Governance

Criminal governance represents a regulatory and procedural framework aimed at protecting public funds and ensuring the effectiveness of criminal justice mechanisms in addressing digital risks, with a particular emphasis on transparency, accountability, and institutional efficiency within public administration (Wikipedia, 2025a).

Within the digital environment, criminal governance requires the integration of legal norms, technological systems, and oversight mechanisms in such a way that artificial intelligence can contribute to the prevention of financial crimes before their occurrence, rather than being limited to punitive intervention after the commission of the offense (Straub, Morgan, Bright, & Margetts, 2022).

#### 2.1.2. The Philosophy of Proactive Prevention

Digital criminal governance reflects a fundamental shift in the philosophy of criminal punishment. The primary objective is no longer retribution after harm has occurred, but rather the establishment of digital safeguards designed to prevent the commission of crimes ab initio (Straub et al., 2022). This philosophy is grounded in the concept of preventive criminal governance, which seeks to bridge the temporal gap between the commission of a crime and its detection, prioritizing anticipatory mechanisms over ex post deterrence.

**A. Real-Time Algorithmic Monitoring**

This approach relies on advanced artificial intelligence systems operating in real time (real-time audit), as opposed to traditional oversight mechanisms that review documents only after the completion of financial transactions. These systems conduct continuous monitoring of public fund flows within digital public procurement processes, enabling the immediate detection of any manipulation of tender specifications or deviations from award criteria. Moreover, they allow for the automated issuance of alerts to the competent judicial authorities (United Nations Office on Drugs and Crime, n.d.; OECD, 2024).

**B. Predictive Analytics and Criminal Pattern Modeling**

Proactive prevention is grounded in the predictive analysis of financial behavior, whereby artificial intelligence examines historical public expenditure data and constructs predictive models capable of identifying risk indicators (*red flags*) prior to the occurrence of embezzlement. This approach facilitates the detection of potential collusion between economic operators and public officials by tracing hidden connections and unjustified financial flows (Kurshan, Mehta, Bruss, & Balch, 2024).

**C. Financial System Hardening**

At the core of proactive prevention lies the transformation of legal rules into technical protocols embedded within digital systems (*automated compliance*). Under this model, any financial operation that violates legal requirements is automatically rejected without human intervention. This mechanism not only limits opportunities for corruption but also reduces the scope of discretionary authority, which is often exploited as an entry point for the misappropriation of public funds. As a result, a more secure and sustainable financial environment is established (Straub & Bright, 2023).

### 2.2. Algeria's Position within International Transformations: Between Sovereignty Challenges and Normative Alignment

Algeria is currently positioned at the heart of a strategic digital transformation that extends beyond the modernization of administrative tools toward a comprehensive reengineering of governance structures. Its engagement in the "Digital Algeria" project and its commitment to the comprehensive digitization

of financial sectors—such as taxation, customs, and state property management—create an urgent need to develop a legal and criminal framework capable of keeping pace with advanced digital systems and responding effectively to artificial intelligence–related risks (Straub, Morgan, Bright, & Margetts, 2022).

2.2.1. The Gap in Alignment with International Standards: The EU AI Act as a Model

While the European Union has made significant progress through the adoption of the EU Artificial Intelligence Act, which classifies AI systems according to levels of risk, Algeria faces a pressing need to adopt similar standards in the management of public funds.

The integration of artificial intelligence systems into the electronic public procurement portal requires their classification as high-risk AI systems, subject to strict human oversight and algorithmic transparency. Such measures are essential to prevent automated deviations that may lead to the dissipation of public resources and to mitigate algorithmic bias against compliant and legitimate economic operators (Straub et al., 2022).

2.2.2. Drawing on the Experiences of Emerging Economies (Brazil and South Korea): Digital Sovereignty

The experiences of South Korea in smart auditing and Brazil in proactive governance provide valuable models for Algeria. These countries have demonstrated that the protection of public funds cannot be achieved solely through ex post criminal deterrence, but rather through technical vigilance systems capable of detecting patterns of cyber fraud within fractions of a second (Kurshan, Mehta, Bruss, & Balch, 2024).

In the Algerian context, the challenge of digital sovereignty serves as a catalyst for the development of national financial oversight algorithms, which may be regarded as a form of financial national security. Reliance on imported technological solutions may expose the state to risks associated with *vendor lock-in*, whereby treasury management becomes dependent on external updates or vulnerable to sudden service disruptions (Straub et al., 2022).

2.3. Toward an Algerian Charter for the Ethics and Governance of Artificial Intelligence

Algeria's ambition is not confined to punitive measures alone; it extends toward the establishment of an integrated digital governance framework that combines modern criminal legislation with proactive technical oversight. The objective is to move from a paradigm focused on prosecuting corrupt actors to one centered on systemic fortification (system hardening).

This approach ensures that the Algerian digital financial system is secure by design, protecting public funds against ransomware attacks and digital identity forgery, while fully respecting personal data protection and citizens' rights, in accordance with international standards of digital human rights (Digital Government Authority, 2025).

2.4. Future Outlook: The Anticipated Legal Framework

It is anticipated that the forthcoming national framework law on artificial intelligence in Algeria—expected to be enacted in the coming years—will constitute a cornerstone of the national digital criminal policy. This legislation is expected to define, for the first time, the concept of virtual legal personality and the limits of human liability for algorithmic errors in financial administration. Such developments would represent a legislative precedent in the regulation of cybercrimes related to public funds (Straub et al., 2022).

## III. Deterrence Policy and the Future of Criminal Protection in Algeria

3.1. The Effectiveness of Traditional Sanctions in Confronting "Intelligent Crime"

Traditional deterrence policy in Algeria is primarily grounded in criminal sanctions provided for under the Penal Code (Law No. 16-01) and the Code of Criminal Procedure, with imprisonment and fines serving as the principal deterrent mechanisms. However, recent studies indicate that AI-enabled digital and financial crimes often surpass the deterrent capacity of such sanctions. This is largely due to the fact that these crimes are perpetrated through autonomous systems or complex algorithms that are difficult

to trace and for which attributing legal responsibility to a clearly identifiable offender proves challenging (Kurshan, Mehta, Bruss, & Balch, 2024).
Moreover, the application of traditional sanctions encounters the dilemma of fragmented criminal liability, as responsibility may lie with the system developer, the end user, or the legal entity itself. This multiplicity of potential offenders renders existing punitive frameworks insufficient to protect public funds from advanced digital threats (Straub, Morgan, Bright, & Margetts, 2022).

3.2. Advanced Digital Criminal Investigation Mechanisms
Confronting what may be described as "algorithms of corruption" necessitates a shift from conventional investigative methods to forward-looking digital criminal investigations that integrate modern technologies into early detection and forensic analysis. Algeria has sought to operationalize this transition by incorporating artificial intelligence and digital analytics into judicial and institutional practices (Straub, Morgan, Bright, & Margetts, 2022).

3.2.1. Specialized Judicial Units and the Challenge of Technical Sovereignty
Algeria has strengthened the role of specialized national judicial units—particularly the Financial and Economic Pole of the Sidi M'Hamed Court—by equipping them with big data analytics laboratories operated by judicial police services, including the National Gendarmerie and the National Police. These tools are designed to dismantle criminal networks that exploit artificial intelligence to conceal the embezzlement of public funds or to launder money through virtual assets (Digital Government Authority, 2025).
**The technical challenge.** The primary obstacle lies in the digital skills gap. Crimes committed using artificial intelligence are characterized by a level of complexity that exceeds the traditional capacities of investigators. Consequently, it has become imperative to train "digital judges" and specialized investigators with expertise in algorithmic analysis, in order to prevent offenders from evading liability under the pretext of "algorithmic error" (Kurshan, Mehta, Bruss, & Balch, 2024; Algerian Ministry of Justice, 2025).

3.2.2. Algorithmic Forensics and Digital Oversight
Contemporary criminal policy increasingly relies on advanced digital investigation models that extend beyond the mere examination of electronic devices to encompass the behavioral analysis of autonomous systems. These mechanisms include:
**A. Digital Forensics**
Tracing transaction logs within public procurement systems and digital taxation platforms to identify any manipulation of databases or unauthorized access to financial information (Straub et al., 2022; OECD, 2024).
**B. Behavioral Deviation Analysis of Systems**
Employing machine learning algorithms to monitor the behavior of public financial management systems. Where an atypical transaction—such as the award of a contract at an unusual time or in violation of algorithmic transparency criteria—is detected, an automated alert is immediately transmitted to judicial oversight authorities (Kurshan et al., 2024).
**C. Virtual Asset Investigation**
With the growing use of cryptocurrencies in bribery schemes and financial manipulation, Algerian authorities have adopted blockchain analysis tools to de-anonymize digital wallets linked to corruption-related offenses. These tools play a critical role in protecting public funds from digital extortion and illicit financial flows (Kurshan et al., 2024).

3.3. A Prospective Vision for the Development of Algerian Legislation: Toward a "Smart Criminal Law"
Emerging algorithmic crimes compel the Algerian legislator to move beyond classical legal approaches and toward a flexible legislative architecture capable of accommodating the fluid and rapidly evolving nature of cyber-enabled offenses targeting public funds (Straub et al., 2022).

3.3.1. Modernizing the Sanctioning and Procedural System: From the Material Offender to the "Virtual Actor"

Digital transformation necessitates a reconfiguration of core criminal law concepts within the Algerian legal system, including:

**A. Humanizing Algorithmic Liability**

This approach entails amending the Penal Code to recognize the "criminal exploitation of intelligent systems" as an aggravating circumstance, while adopting the concept of "liability for algorithmic output." Under this framework, criminal responsibility may be attributed to the legal entity (corporation) or the software developer where probabilistic intent or gross negligence in security standards can be established (Straub et al., 2022).

**B. Digital Jurisdiction**

Given the cross-border nature of artificial intelligence–related crimes, amendments to the Code of Criminal Procedure are anticipated to facilitate electronic letters rogatory and direct cooperation with cloud service providers. Such measures would ensure the rapid preservation of digital evidence before it is erased or encrypted (United Nations Office on Drugs and Crime, n.d.).

3.3.2. Institutionalizing Preventive Governance: Financial Security "by Design"

The focus of criminal policy is thus expected to shift from deterrence toward prevention through the technical institutionalization of criminal governance, encompassing:

**A. The National Observatory for Digital Ethics**

A technical advisory body affiliated with the High Authority for Transparency, tasked with auditing the fairness and integrity of algorithms used in public procurement and taxation systems, and ensuring that no vulnerabilities exist that could facilitate algorithmic bias or automated embezzlement.

**B. Early Warning Algorithmic Systems**

Mandating public financial institutions to integrate criminal vigilance software alongside payment systems, enabling the automatic detection and freezing of anomalous spending patterns, and the immediate notification of the public prosecutor (Kurshan et al., 2024).

**C. Normative Alignment and Digital Sovereignty**

The formulation of legal frameworks for digital financial security grounded in the philosophy of data sovereignty, whereby Algeria's sensitive financial data are stored within a national cloud infrastructure subject exclusively to Algerian law. At the same time, transparency principles inspired by the EU AI Act are incorporated to enhance the credibility of these systems vis-à-vis investors and international economic operators (Straub et al., 2022).

## IV. Conclusion and Recommendations

### 4.1. Summary of Findings

The study confirms that Algeria's comprehensive digital transformation, marked by the integration of generative artificial intelligence and predictive algorithms into public financial management, has opened new horizons for expenditure rationalization and enhanced transparency. However, this transformation has simultaneously generated unprecedented criminal risks characterized by *"intelligence and abnormality"*, particularly in the form of algorithmic manipulation, automated decision abuse, and digitally mediated misappropriation of public funds (Straub, Morgan, Bright, & Margetts, 2022).

The findings highlight several key conclusions:

**a. Limitations of the Traditional Algerian Criminal Framework**

The current Algerian criminal legislation, grounded in classical concepts of criminal liability based on free will and the involvement of a natural offender, proves inadequate to address complex algorithm-driven crimes. Existing sanctions and liability rules fail to capture the diffuse, opaque, and multi-actor nature of algorithmic offenses affecting public funds (Kurshan, Mehta, Bruss, & Balch, 2024).

**b. Preventive Criminal Governance as a Strategic Solution**

Shifting from ex post punitive deterrence to proactive digital oversight significantly enhances the protection of public funds and enables early detection of financial risks. Nevertheless, this preventive governance approach remains insufficiently developed and underutilized within the current Algerian legal framework (Digital Government Authority, 2025).

**c. Algeria's International Position and Sovereignty Challenges**

The adoption of nationally developed financial oversight algorithms strengthens public fund protection and reinforces digital financial security. However, such an approach requires careful alignment with international regulatory standards—most notably the EU Artificial Intelligence Act—while preserving Algeria's sovereign legal and constitutional choices (Straub et al., 2022).

### 4.2. Strategic Recommendations

Based on the comprehensive analysis of the current and future trajectories of Algerian criminal policy in the digital age, the study proposes a set of strategic recommendations structured across four complementary levels:

**a. Legislative Reforms**

- **Enactment of a Framework Law on Artificial Intelligence**
  The Algerian legislator is urged to adopt a comprehensive AI framework law defining the legal nature of intelligent systems and establishing joint criminal liability among programmers, system owners, and users for algorithmic acts that harm public funds. The introduction of *"gross programming fault"* as an aggravating circumstance is also recommended (Straub et al., 2022; Kurshan et al., 2024).
- **Modernization of Substantive and Procedural Criminal Law**
  The Criminal Code should be revised to include newly emerging offenses such as *"algorithmic fraud"* and *"financial digital identity falsification."* In parallel, the Code of Criminal Procedure should be amended to grant judges explicit powers for cloud-based searches, real-time seizure of digital assets, and the freezing of cryptocurrencies linked to public fund offenses (OECD, 2024; Algerian Ministry of Justice, 2025).

**b. Institutional Strengthening**

- **Institutionalization of a National Observatory for Digital Ethics**
  Establishing an independent national body tasked with algorithmic criminal auditing in sensitive financial sectors is essential to ensure the absence of bias, manipulation, or exploitable vulnerabilities within deployed systems (Straub & Bright, 2023).
- **Investment in the "Digital Judge" Concept**
  Specialized training programs should be introduced for national criminal judicial units in the field of algorithmic forensics, enabling judges and prosecutors to effectively investigate and adjudicate highly complex cyber-financial crimes (Kurshan & Mehta, 2023).

**c. Technical Measures**

- **Deployment of Supervisory Artificial Intelligence (SupTech)**
  The adoption of AI-powered early warning systems to monitor national financial transactions is recommended, allowing for anomaly detection and the automatic suspension of suspicious operations before material harm occurs (OECD, 2024).
- **Implementation of Algorithmic Sovereignty (Sovereign AI)**
  Developing national algorithms for managing and analyzing large-scale financial data is critical to avoiding vendor lock-in risks and ensuring the protection of the State's sensitive financial information (Straub et al., 2022; Kurshan et al., 2024).

**d. Future-Oriented Perspectives**

- **Adoption of the "Security by Design" Philosophy**
  Criminal policy should evolve from a reactive sanction-based approach to a preventive digital hardening strategy, whereby technical prevention becomes an integral component of criminal governance (United Nations Office on Drugs and Crime, n.d.).
- **Active Normative Alignment**

Continuous engagement with international best practices—such as the EU AI Act and the experiences of Asian digital leaders—should be pursued, while ensuring contextual adaptation consistent with Algeria's constitutional, cultural, and sovereign specificities, thereby safeguarding citizens' digital rights alongside public funds (European Commission, 2023; Straub & Bright, 2023).

**Final Conclusion**

The study concludes that the protection of public funds in Algeria in the era of artificial intelligence cannot be confined to post-offense punishment. Rather, it necessitates a multidimensional preventive criminal governance framework encompassing legislation, technology, and institutional reform. Integrating artificial intelligence into financial oversight mechanisms, while ensuring strict adherence to ethical and legal standards, constitutes a decisive step toward building a secure, sustainable digital financial system capable of confronting sophisticated cyber threats and preserving national digital sovereignty.

**References**


European Commission. (2023). *Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

Digital Government Authority. (2025). *Generative artificial intelligence in digital government operations: Good governance practices*. Ministry of Communications and Information Technology. https://dga.gov.sa/ar/digital-knowledge/GenAI-in-digital-government

Algerian Digital Government Authority. (2023). *Digital Algeria project: Digital financial governance of public funds*. Ministry of Finance of Algeria. https://www.mf.gov.dz/digital-transformation

Kurshan, E., Mehta, D., Bruss, B., & Balch, T. (2024). AI is turbocharging organized crime: Financial crime trends and AI implications. *Journal of Financial Crime & Technology*. https://doi.org/10.1108/JFCT-03-2024-0056

Kurshan, E., & Mehta, D. (2023). Cybercrime, AI, and financial governance: Emerging threats and global best practices. *Journal of Financial Crime, 30*(4), 1123–1145. https://doi.org/10.1108/JFC-03-2023-0056

Organisation for Economic Co-operation and Development. (2024). *AI in public sector governance: Opportunities and challenges*. OECD Publishing. https://www.oecd.org/going-digital/publications/ai-in-public-sector.htm

Organisation for Economic Co-operation and Development. (2024). *Digital forensics and anti-corruption: Emerging trends in public procurement*. OECD Publishing. https://www.oecd.org/gov/digital-forensics-anti-corruption.htm

Straub, V. J., Morgan, D., Bright, J., & Margetts, H. (2022). *Artificial intelligence in government: Concepts, standards, and a unified framework*. Oxford Internet Institute. https://arxiv.org/abs/2210.17218

Straub, V. J., & Bright, J. (2023). Ethics and accountability in AI-driven government systems. *Government Information Quarterly, 40*(1), 101–117. https://doi.org/10.1016/j.giq.2022.101117

United Nations Development Programme. (2022). *Digital governance for sustainable public finance: Case studies and lessons learned*. https://www.undp.org/publications/digital-governance-sustainable-public-finance

United Nations Office on Drugs and Crime. (n.d.). *United Nations standards on crime prevention and criminal justice*. https://www.unodc.org/e4j/ar/anti-corruption/module-4/key-issues/references.html

Ministry of Justice (Algeria). (2025). *Judges' guide on handling digital evidence and emerging cybercrimes*. Algiers: Ministry of Justice.