

The Integration of Artificial Intelligence and Cyber security in Supporting Suspicious Transaction Reporting to Combat Money Laundering.

دمج الذكاء الاصطناعي والأمن السيبراني في دعم الإبلاغ عن المعاملات
المشبوكة لمكافحة غسل الأموال.

MALKI Toufik

مالكي توفيق

Research Lab in legal and economic sciences, مخبر الأبحاث في العلوم القانونية والاقتصادية

University of Tissemsilt, Algeria.

جامعة تيسمسيلت - الجزائر

Malki.Toufik@yahoo.fr

Malki.Toufik@yahoo.fr

Submission date: 20/09/2025

Date of acceptance: 12/10/2025

ABSTRACT:

ملخص باللغة العربية:

Money laundering poses a threat to financial stability by channeling illicit funds into the legitimate economy. Suspicious transaction reporting is a core anti-money laundering tool, but its effectiveness is currently challenged by complex crimes and digital vulnerabilities. This article examines how Artificial Intelligence can enhance detection and how cyber security secures reporting platforms. It reviews Algerian legislation within international standards and concludes with recommendations to strengthen the national framework.

يشكل غسل الأموال أحد أبرز التحديات التي تهدد المنظومة المالية لما يتيح من إدماج للأموال غير المشروعة في الدورة الاقتصادية. ويبرز نظام الإخطار بالعمليات المشبوهة كآلية أساسية لمكافحته، غير أن فعاليتها تتراجع أمام تعقد الأساليب الإجرامية وضعف الحماية الرقمية. يركز المقال على توظيف الذكاء الاصطناعي لتحسين دقة الرصد، وعلى دور الأمن السيبراني في تأمين منصات الإبلاغ، مع عرض التجربة الجزائرية في ضوء المعايير الدولية وتقديم توصيات لتقوية الإطار التشريعي والمؤسسي

Keywords: Money laundering; Suspicious Transaction Reporting; Artificial Intelligence; Cyber security; Algerian legal framework

كلمات مفتاحية: غسل الأموال؛ الإبلاغ عن المعاملات المشبوهة؛ الذكاء الاصطناعي؛ الأمن السيبراني؛ الإطار القانوني الجزائري.

Introduction:

Money laundering has long been recognized as one of the most serious threats to the integrity and stability of national and international financial systems. By disguising the illicit origin of funds, criminal networks succeed in integrating illegal proceeds into the legal economy, thereby undermining transparency, weakening trust in financial institutions, and facilitating the expansion of organized crime and terrorism. To address this phenomenon, legal systems have progressively adopted preventive measures, among which Suspicious Transaction Reporting occupies a central place. Through this mechanism, financial and non-financial entities are legally required to report operations that raise reasonable suspicion of criminal activity, thus allowing competent authorities to intervene before illicit funds are fully integrated into the economy, but the effectiveness of suspicious transaction reporting is increasingly challenged by two factors. On the one hand, the complexity and sophistication of laundering techniques make it difficult for traditional monitoring systems to detect suspicious patterns with precision. On the other hand, the digitalization of financial services has exposed reporting platforms to cyber threats that risk compromising the confidentiality, integrity, and reliability of transmitted data. These challenges highlight the necessity of integrating Artificial Intelligence and cyber security into the legal and institutional framework of suspicious transaction reporting, ensuring that the duty to report is both effectively implemented and securely protected.

The importance of this topic is particularly evident in Algeria, where the national legal framework, established by Law No. 05-01 of 2005 on the prevention of money laundering and the financing of terrorism and its subsequent amendments, reflects the country's adherence to international conventions and the recommendations of the Financial Action Task Force

(FATF). So, like many jurisdictions, Algeria faces difficulties in translating legal obligations into effective practice, especially in the face of growing digital risks and the need for modern detection tools.

This research is guided by the following problematic question:

To what extent can the integration of Artificial Intelligence and cyber security enhance the effectiveness of suspicious transaction reporting in combating money laundering within the Algerian legal framework?

For that reason, this study aims to clarify the legal framework governing suspicious transaction reporting, to analyze the added value of Artificial Intelligence in detecting illicit financial activities, and to highlight the role of cyber security as a safeguard for the reporting chain. By doing so, it seeks to propose practical recommendations to strengthen Algeria's capacity to prevent and combat money laundering in conformity with international standards while preserving the principles of legality, confidentiality, and data protection

THE FIRST TOPIC

Artificial Intelligence as a Tool to Strengthen Suspicious Transaction Reporting

This chapter explores both the regulatory foundation of suspicious transaction reporting and the contribution of Artificial Intelligence to improving its effectiveness

First Requirement:

The legal and regulatory framework of Suspicious Transaction Reporting in Anti-Money Laundering.

Suspicious Transaction Reporting has emerged as a fundamental pillar of the global anti-money laundering system, functioning as a preventive mechanism to safeguard the integrity of the financial sector. The notion of STR is grounded in the obligation of financial institutions, and increasingly of non-financial entities, to report any transaction that raises reasonable suspicion of being connected to criminal activity, even in the absence of definitive proof¹ This obligation reflects the principle that timely detection and communication of unusual or unexplained financial behavior can disrupt the laundering cycle at its earliest stages, thereby strengthening the preventive capacity of the law .

At the international level, the legal foundation of STR is anchored in several landmark instruments. The 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention)² was the first to explicitly recognize the need for states to adopt measures for detecting and reporting transactions suspected of being linked to drug-related money laundering³. This obligation was later expanded through the 2000 United Nations Convention against Transnational Organized Crime (Palermo Convention), which

1 Financial Action Task Force. (2020). COVID-19-Related Money Laundering and Terrorist Financing: Risks and Policy Responses. Official Report, paris.

2 Nations, U. (1988, December 20). United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances. Vienna.

3 Sorour, A. F. (2003). Money Laundering and Terrorist Financing. Cairo: Dar Al-Nahda Al-Arabiya pp 8-9.

extended reporting requirements to all serious crimes generating illicit proceeds, thereby broadening the scope of STR obligations. The 2003 United Nations Convention against Corruption reinforced this framework by stressing the importance of suspicious transaction reporting as a preventive measure against corruption and associated money laundering practices¹. Complementing these conventions, the Financial Action Task Force (FATF) has played a decisive role in shaping a global standard. Its 40 Recommendations, which have become the benchmark for AML compliance worldwide, place STR at the center of national AML regimes. Recommendation 20 specifically requires financial institutions to report promptly to the Financial Intelligence Unit when they suspect or have reasonable grounds to suspect that funds are linked to, or intended for, criminal activity². Recommendation 21 further ensures that institutions and employees making such reports are granted protection from liability and are prohibited from “tipping off” clients. These principles not only harmonize obligations across jurisdictions but also emphasize confidentiality, accountability, and cooperation between the private sector and state authorities.

At the regional level, frameworks such as the European Union’s Anti-Money Laundering Directives have progressively refined the scope and implementation of STR duties. Beginning with the First Directive in 1991, which required financial institutions to identify clients and report suspicious transactions, successive directives expanded both the range of obligated

1 Nations, U. (2000, November 15). Palermo Convention. United Nations Convention against Transnational Organized Crime. New York.

2 RECOMMENDATIONS, F. A. (2012). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. Retrieved 06 13, 2025, from :
www.fatf-gafi.org/recommendations.htm

entities and the definition of suspicious activity. The Fourth AMLD (2015) and Fifth AMLD (2018) introduced stricter customer due diligence standards, obliged member states to create centralized registers of beneficial ownership, and reinforced mechanisms for cooperation among FIUs¹. The Sixth AMLD (2018/2019) went further by harmonizing the definition of money laundering offenses across the EU and strengthening sanctions for non-compliance with reporting duties. These developments demonstrate the dynamic evolution of the STR framework in response to increasingly sophisticated laundering schemes².

At the national level, most jurisdictions have translated these international and regional obligations into comprehensive anti-money laundering statutes. For instance, the United States enacted the USA PATRIOT Act (2001)³, which reinforced the Bank Secrecy Act by obliging financial institutions to implement customer due diligence measures and file Suspicious Activity Reports with the Financial Crimes Enforcement Network. In the United Kingdom, the Proceeds of Crime Act (2002) introduced wide ranging obligations on banks, accountants, and legal professionals to submit STRs whenever they suspect that property or funds may represent criminal

1 Fourth AMLD.05-01, A. 2.–2. (2005, feb 06). The prevention of money laundering and financing of terrorism. Algeria. 2015/849, D. (. (2015, may 20). Fourth AMLD.

2 Sixth AMLD/2018 1673, D. (. (2018, October 23).

3 Daoud, M. M. (2022). A proposed framework for studying the impact of cyber security on accounting information to increase trust in the financial reports in the context of industry 4.0: An event, impact and response approach. The Sixth Scientific Conference of the Faculty of Commerce. 42, pp. 20-61. Syria: Tanta University.

proceeds¹. Within the European Union, member states have successively transposed the AML Directives into domestic law, progressively enlarging the scope of reporting entities and standardizing penalties for non-compliance. These national frameworks, although varied in form, share the common principle of imposing a legal duty to report suspicious transactions promptly to the competent FIU².

Failure to comply with these obligations often triggers significant consequences, ranging from administrative sanctions and heavy fines to potential criminal liability for both institutions and individuals. At the same time, legal systems generally recognize the importance of safe harbor provisions, which shield institutions and employees from liability when they report in good faith, even if subsequent investigations prove the suspicion to be unfounded. Another central element is the strict prohibition of “tipping-off,” which prevents institutions from disclosing to clients that a report has been filed against them, thereby protecting the integrity of ongoing investigations. Despite the apparent robustness of this multi layered framework, critical challenges persist³. In certain jurisdictions, the number of reports submitted is disproportionately low, reflecting either a lack of awareness or a fear of legal repercussions among reporting entities. Conversely, in other jurisdictions, over-reporting has created a flood of low quality STRs that overwhelm FIUs and dilute their analytical capacity. Confidentiality concerns also remain pressing: while FIUs are mandated to safeguard data, the sheer volume of sensitive

1 Kingdom, U. (2002, 07 24). Proceeds of Crime. POCA 2002. London: The Stationery Office.

2 CHAWKI, M. e. (2015). Cybercrime, Digital Forensics and Jurisdiction. Springer, p03.

3 Articles 21–23 (2005). Law No. 05-01. Algeria.

financial information collected through STRs raises legitimate questions about privacy, data protection, and potential misuse. Also, the effectiveness of STR obligations is often undermined by resource disparities between countries, as not all FIUs possess the technological tools or trained personnel necessary to analyze complex patterns of suspicious activity. Another pressing issue lies in the transnational nature of money laundering, which often outpaces the capacity of national frameworks. Although mechanisms such as the Egmont Group facilitate international cooperation, differences in legal definitions, thresholds for suspicion, and levels of enforcement still create loopholes that sophisticated criminal networks can exploit. These discrepancies highlight the need for greater harmonization of legal standards and stronger information sharing protocols between jurisdictions¹.

Second Requirement:

The Contribution of Artificial Intelligence in Detecting Suspicious Financial Transactions

In Algeria, the obligation to report suspicious financial operations is legally grounded in Law No. 05-01 of 6 February 2005 relating to the prevention of money laundering and the financing of terrorism, as amended and supplemented by Law No. 15-06 of 20 July 2015². These legislative instruments clearly stipulate that financial institutions, insurance companies, and certain non-financial professions are required to submit declarations of suspicion whenever they detect operations that may involve money laundering or terrorism financing. The competent authority for receiving such declarations is the Cellule de Traitement du Renseignement Financier, established

1 Sorour, A. F. op Cit , p 11

2 Article. 1. 01-05 (2005). the Prevention of Money Laundering and the Financing of Terrorism.

as an independent administrative body responsible for collecting, analyzing, and transmitting financial intelligence to judicial and security institutions. Executive Decrees, notably Decree No. 12-02, have further specified the CTRF's prerogatives, its independence, and its role in implementing the FATF recommendations at the domestic level¹.

The Algerian legal framework also provides a set of safeguards and obligations surrounding suspicious transaction reporting. The law prohibits "tipping-off," ensuring that clients are not alerted when a report is filed against them. Institutions and employees who declare suspicious operations in good faith enjoy immunity from liability, while those who fail to report may face administrative penalties, substantial fines, or criminal prosecution². These provisions reflect Algeria's compliance with the Vienna Convention of 1988, the Palermo Convention of 2000, and the United Nations Convention against Corruption of 2003, all of which Algeria has ratified and incorporated into its domestic legal order. But, despite this robust legislative framework, the practical implementation of suspicious transaction reporting in Algeria and elsewhere faces serious challenges. Traditional compliance systems often rely on static rules, fixed thresholds, and manual verification, which generate large volumes of alerts with limited discriminatory value. This phenomenon, sometimes referred to as "over reporting," risks overwhelming the CTRF with low quality information, reducing its capacity to focus on genuinely suspicious activities. Conversely, the absence of advanced detection mechanisms may also result in under reporting, where significant laundering operations remain unnoticed due to the inability of institutions to

1 CHAWKI, M. e, op Cit ,p 5.

2 MOLANDER, R. C., MUSSINGTON, D., & WILSON, P. A. (1998). Cyber payments and Money Laundering: Problems and Promise. unites state: RAND Corporation's, p 11.

detect sophisticated patterns¹. It is in this context that Artificial Intelligence offers significant contributions to the process of suspicious transaction detection. Through machine learning and data analytics, AI systems can process vast volumes of financial data in real time, identify anomalies that deviate from a customer's usual financial behavior, and highlight patterns that correspond to the legal criteria of suspicion under Algerian law. For example, algorithms can detect structured deposits designed to avoid reporting thresholds, repeated transfers to high risk jurisdictions, or unusual movements of funds through intermediaries in real estate or trade operations scenarios frequently associated with laundering techniques². Also, AI enhances the analytical capacity of the CTRF by supporting cross referencing of information obtained from different national bodies such as customs, tax authorities, and commercial registries. Article 18 of Law 05-01 explicitly empowers the CTRF to request information from various public authorities; AI tools strengthen this prerogative by enabling the systematic integration and analysis of diverse datasets, thus producing intelligence of higher quality and greater investigative value³. So the introduction of AI into AML compliance frameworks must be aligned with the principles of legality, proportionality, and due process. Reports generated by automated systems cannot replace the responsibility of compliance officers and financial institutions as outlined in Article 21 of Law 05-01, which entrusts them with the task of verifying and transmitting suspicious transaction reports. Human oversight remains indispensable to ensure that AI alerts are legally relevant, contextually accurate, and compatible with the guarantees of

1 MOLANDER, R. C., MUSSINGTON, D., & WILSON, P. A, op. Cit , p 12 2308/91 /EEC, C. D. (1991, June 10). prevention of the use of the financial system for the purpose of money laundering.

3 Article 18 (2005). Law No. 05-01. Algeria.

confidentiality and data protection established under Algerian law and international standards¹.

The practical implementation of Suspicious Transaction Reporting mechanisms represents the operational dimension of the legal obligations established at both the international and domestic levels. While conventions, FATF recommendations, and national legislation define the duty to report, its effectiveness ultimately depends on the clarity of procedures, the role of institutions involved, and the guarantees afforded to reporting entities². In Algeria, the modalities of STR are clearly laid out in Law No. 05-01 of 6 February 2005, as amended by Law No. 15-06 of 2015, and its implementing decrees. Under these provisions, the process begins at the level of financial and non-financial reporting entities, such as banks, insurance companies, real estate agencies, notaries, and auditors, which are legally bound to monitor their clients' transactions and submit declarations of suspicion whenever reasonable grounds exist to believe that an operation may be linked to money laundering or terrorist financing. The declaration is filed with (the Cellule de Traitement du Renseignement Financier), which serves as the national Financial Intelligence Unit³. The submission procedure requires institutions to complete a standardized declaration form, detailing the identity of the client, the nature of the suspicious transaction, and the reasons justifying the suspicion. These reports must be transmitted promptly, without delay, to prevent the possible disappearance or integration of illicit funds into the legitimate economy. Importantly, Algerian legislation prohibits "tipping-off,"

1 Article 21 (2005). Law No. 05-01. Algeria.

2 A. 2.-2 05-01, . (2005, feb 06). The prevention of money laundering and financing of terrorism. Algeria.

3 RECOMMENDATIONS, F. A. (2012). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, op Cit , p17.

meaning that clients cannot be informed that a suspicious report has been filed against them, thereby preserving the confidentiality and integrity of ongoing investigations. Once received, the CTRF conducts an initial analysis to assess the seriousness and relevance of the reported suspicion. In this phase, the CTRF has the authority, pursuant to Article 18 of Law No. 05-01¹, to request additional information from other state authorities such as tax administrations, customs, commercial registries, or even directly from the reporting institution. If the suspicion is confirmed, the CTRF forwards the case to the competent judicial authorities for further investigation and potential prosecution.

Internationally, similar procedures are reflected in the practices of other jurisdictions. In the United States, financial institutions are required to file Suspicious Activity Reports with the Financial Crimes Enforcement Network within 30 days of detecting suspicious activity. In the European Union, national FIUs operate under harmonized rules derived from successive AML Directives, ensuring consistency in reporting requirements across member states. These comparative practices highlight that, while procedural details may differ, the essential elements of rapid reporting, confidentiality, immunity for reporters, and sanctions for non-compliance remain common to most legal systems². In practice, the effectiveness of STR systems depends not only on the legal framework but also on the professional training of compliance officers, the adoption of technological tools to monitor transactions, and the capacity of FIUs to analyze and act upon the reports they receive. Algeria, in this respect, has made significant progress by reinforcing the

1 Financial Action Task Force. COVID-19-Related Money Laundering and Terrorist Financing: Risks and Policy Responses. Op Cit.

2 CHAWKI, M. e, op Cit ,p 7.

prerogatives of the CTRF and by integrating its work with international cooperation mechanisms such as the Egmont Group. But, ongoing challenges such as the need for continuous training, modernization of reporting tools, and better coordination between the financial sector and state institutions remain central to enhancing the quality and timeliness of STRs¹

THE SECOND TOPIC

Cyber security as a Safeguard for Suspicious Transaction Reporting Systems

This chapter examines the threats that may compromise reporting systems and highlights the role of cyber security, in conjunction with technological tools, in preserving the integrity of the anti-money laundering framework

First Requirement:

Cyber Threats to Financial Reporting Systems

Suspicious Transaction Reporting frameworks, while legally robust, remain highly vulnerable to cyber threats that target the financial sector. The digitization of financial services has significantly increased the attack surface for criminals, who now exploit weaknesses in information and communication technologies to circumvent reporting obligations or manipulate data. Cybercrime and money laundering have thus become increasingly intertwined, requiring legal systems to address not only the substantive obligation to report suspicious transactions but also the security of the digital infrastructures supporting this

1 MOLANDER, R. C., MUSSINGTON, D., & WILSON, P. A, op. Cit , pp. 12-13.

obligation¹. As in many jurisdictions, the Algerian law on cybercrime (Law No. 09-04 of 5 August 2009 on specific rules relating to the prevention and fight against offences connected with information and communication technologies) complements AML legislation by criminalizing unauthorized access to information systems, data manipulation, and the use of digital platforms for illicit purposes. This law provides the legal basis for prosecuting cyber activities that could compromise the confidentiality and integrity of suspicious transaction data. When combined with Law No. 05-01 on AML/CFT, these provisions establish a dual framework in which suspicious reporting is not only mandatory but also protected against electronic interference².

Cyber threats to STR systems can take various forms. Unauthorized access to reporting platforms may allow criminals to detect ongoing investigations or intimidate reporting entities. Data breaches can result in the leakage of sensitive financial intelligence, exposing both institutions and individuals to risks. Manipulation of data within reporting systems may lead to the alteration or deletion of suspicious declarations, directly undermining the effectiveness of AML frameworks. Besides that, ransom ware attacks on financial institutions can paralyze monitoring systems, creating a window of opportunity for laundering activities to proceed undetected³.

1 WALL, D. S. (2007). Policing cybercrimes: Situating the public police in networks of security within cyberspace. *Police Practice and Research*, 2(8), 187.

2 Idem, p188

3 Article 01 No. 47, (5 August 2009). laying down specific rules relating to the prevention and fight against offences connected with information and communication technologies. Algeria: Official Journal of the People's Democratic Republic of Algeria. P05.

The FATF has repeatedly emphasized the risks posed by cybercrime to AML regimes, urging states to ensure the confidentiality, integrity, and timely transmission of suspicious transaction reports. Also, the European Union's General Data Protection Regulation imposes strict requirements for data protection in the financial sector, ensuring that personal data collected for AML purposes is secured against cyber risks. These standards are highly relevant for Algeria¹, where growing digitalization of financial services requires parallel investment in cyber security frameworks to guarantee the reliability of STR mechanisms. The vulnerability of STR systems to cyber threats demonstrates that legal obligations alone are insufficient without a protective technological environment. For this reason, cyber security has become an integral safeguard, ensuring that the transmission, storage, and analysis of suspicious transaction data remain credible, confidential, and resistant to malicious interference. In practical terms, this means that the entire reporting chain from the compliance officer in a financial institution to the national Financial Intelligence Unit must operate within a secure digital infrastructure². Without such protection, even the most comprehensive laws risk being undermined by technical weaknesses that allow criminals to intercept, alter, or destroy sensitive financial information. As well, cyber security ensures that trust in the reporting system is preserved. Financial institutions are more likely to comply fully with their reporting obligations when they have confidence that the information they submit will be securely handled and protected from leakage. Likewise, FIUs depend on the confidentiality and integrity of digital channels to maintain cooperation with both domestic institutions and international partners. For Algeria, where the CTRF plays a central role in the

1 Ibid.

2 WALL, D. S, op Cit ,pp. 188-189.

AML/CFT framework, strengthening cyber security capacities has become not only a technical necessity but also a legal imperative to guarantee the reliability of suspicious transaction reporting as envisaged by Law No. 05-01 and its subsequent amendments¹

Second Requirement:

Securing Suspicious Transaction Reporting

The effectiveness of Suspicious Transaction Reporting depends not only on the existence of a legal obligation to declare suspicious operations, but also on the ability of institutions to detect them accurately and transmit them securely. Law No. 05-01 of 6 February 2005 relating to the prevention of money laundering and the financing of terrorism, as amended by Law No. 15-06 of 20 July 2015, clearly establishes the duty of banks, financial institutions, and certain non-financial professions to report operations suspected of involving illicit funds². Article 21 of the law entrusts these entities with the responsibility of verifying and transmitting suspicious reports, while Article 18 empowers the Financial Intelligence Unit to request any complementary information necessary for its analysis³. These provisions demonstrate that detection and protection are two inseparable pillars of the reporting process, so that artificial intelligence provides a powerful contribution to the first pillar by allowing financial institutions to identify suspicious

1 Opuđu, D. O. (2024). Client confidentiality, data privacy and suspicious transactions reporting: the accountant's ethical dilemma in the Nigerian professional space. *UBS Journal of Business and Economic Policy*, 1(2), p113

2 OF QUEBEC, S., & FORTIN, F. (2013). *Cybercrime: Between misconduct and organized crime*. Presses inter Polytechnique. P03

3 OF QUEBEC, S., & FORTIN, F, op Cit , pp. 3-4.

transactions with greater precision. Algorithms based on machine learning can process large volumes of operations, highlight anomalies such as structured deposits or transfers inconsistent with a client's declared activity, and refine the quality of declarations submitted to the competent authority. This technological contribution directly supports the obligation created by Articles 18 and 21, ensuring that reports are not only transmitted but also based on reliable and relevant indicators of suspicion¹.

Cyber security, in turn, guarantees the protection of this reporting chain. Article 38 of Law No. 05-01 criminalizes any act of disclosure or obstruction in relation to suspicious transaction reporting, while Law No. 09-04 of 5 August 2009 on cybercrime punishes unauthorized access to information systems and manipulation of data. The integration of cyber security measures such as encryption, secure authentication, and confidentiality protocols ensures that declarations are transmitted to the Financial Intelligence Unit without risk of interception or alteration. In this way, cyber security acts as the practical shield that secures the legal obligation, preventing any interference that could undermine the integrity of suspicious transaction reporting. This integration is further consolidated by the obligation of confidentiality imposed on all persons involved in the reporting process. The prohibition of "tipping-off," established in Article 22 of Law No. 05-01², reflects the legislator's awareness that the protection of information is as crucial as its detection. Artificial Intelligence strengthens this

1 Daoud, M. M. (2022). A proposed framework for studying the impact of cyber security on accounting information to increase trust in the financial reports in the context of industry 4.0: An event, impact and response approach. The Sixth Scientific Conference of the Faculty of Commerce. 42, pp. 20-61. Syria: Tanta University. P26

2 Article 22 (2005). Law No. 05-01. Algeria.

confidentiality by enabling automated monitoring systems that minimize human handling of sensitive data, while cyber security ensures that the digital platforms used to transmit and analyze reports remain inaccessible to unauthorized actors. By linking the technological capacities of Artificial Intelligence with the legal guarantees of cyber security, suspicious transaction reporting is reinforced as both a legal and technical process. Detection through intelligent systems ensures compliance with the duty to declare, while protection through secure infrastructures guarantees the credibility and confidentiality of the reports. This dual integration transforms the reporting mechanism from a simple legal formality into an operational tool capable of fulfilling the preventive objectives set out by Algerian law in the fight against money laundering and terrorism financing¹

The protection of personal data and the preservation of confidentiality constitute essential guarantees for the credibility of Suspicious Transaction Reporting. Without clear legal safeguards, reporting entities may hesitate to declare suspicious operations for fear of legal consequences, and individuals may lose confidence in the financial system if their data is misused². For this reason, Algerian legislation has given particular importance to both confidentiality and data protection in the context of money laundering prevention³.

Law No. 05-01 of 6 February 2005, amended by Law No. 15-06 of 20 July 2015, provides several guarantees in this

1 Emmanuel, A. A. (2025). The impact of cyber security on financial reporting: Strengthening data integrity and. International Journal of Science and Research Archive, 02(14), p630

2 Opudu, D. O., op Cit ,p 112

3 Nour, B. A. (2022). The impact of ICT on the money laundering crime. Critical Journal of Law and Political Science, 17(1), p1052.

regard. Article 22 explicitly prohibits “tipping-off,” meaning that no employee of a reporting institution may inform a client that a declaration of suspicion has been filed against them. This prohibition ensures that on-going investigations are not compromised and reflects a fundamental principle of the suspicious transaction reporting system: the confidentiality of both the report and the identity of the reporting entity. Article 23 reinforces this obligation by subjecting any disclosure of information relating to suspicious reports to penal sanctions. The law also establishes protections for reporting entities. Employees and institutions that submit reports in good faith enjoy immunity from civil and criminal liability, even if subsequent investigations demonstrate that the suspicion was unfounded¹. This legal immunity encourages compliance and ensures that the duty to report does not become a source of legal risk for those who act responsibly. In this way, data protection and confidentiality are not only safeguards for clients but also mechanisms that strengthen the willingness of institutions to cooperate. Even so, Algeria has adopted a broader legislative framework for personal data protection. Law No. 18-07 of 10 June 2018 relating to the protection of individuals in the processing of personal data establishes general principles of legality, proportionality, and purpose limitation. Although this law has a general scope, its provisions apply directly to the financial sector, where sensitive personal and financial information is processed for suspicious transaction reporting. Article 4 requires that data processing respect the principle of necessity, and Article 8 stipulates that personal data must be secured against unauthorized access or alteration. These provisions align with the obligations of confidentiality contained

¹ Ibid.

in Law No. 05-01, creating a coherent legal framework for the protection of data in AML procedures¹.

The convergence of suspicious transaction reporting and data protection law demonstrates that the fight against money laundering cannot be separated from the protection of individual rights. On the one hand, reporting entities are obliged to transmit detailed personal and financial data to the Cellule de Traitement du Renseignement Financier; on the other, the CTRF and competent authorities must guarantee that this data is processed exclusively for the purposes defined by law and protected against misuse. The balance between security and rights is therefore achieved through the combination of strict confidentiality obligations, legal immunity for reporters, and general rules on data protection. In practice, the implementation of these guarantees requires not only legal provisions but also technical measures. Confidentiality protocols, restricted access to databases, encryption of transmitted data, and secure archiving systems are indispensable to ensure compliance with Articles 22 and 23 of Law No. 05-01 and the general principles of Law No. 18-07. By integrating such measures, Algeria ensures that suspicious transaction reporting remains both a powerful tool in the prevention of money laundering and a process that respects the rights of individuals whose data is processed²

Conclusion:

The study has demonstrated that suspicious transaction reporting is a cornerstone of anti-money laundering frameworks, relying on a dual foundation of legal obligations and

1 Nour, B. A., op Cit , p 1057.

2 Nour, B. A., op Cit , p 1058.

technological support. The integration of Artificial Intelligence and cyber security enhances both the accuracy of detecting suspicious operations and the protection of sensitive financial data. In the Algerian legal system, the combination of Law No. 05-01, Law No. 15-06, and complementary legislation on cybercrime and data protection establishes a comprehensive framework that aligns with international standards while addressing national specificities. Nevertheless, the analysis has also revealed that legal texts alone are insufficient without effective implementation, adequate institutional capacity, and the incorporation of modern technologies.

Based on the findings of this research, several proposals may be advanced:

- 1.Enhancing the institutional capacity of the CTRF and other competent authorities by providing greater independence, resources, and training for personnel, thus enabling more effective analysis of the increasing volume of reports.
- 2.Promoting the adoption of Artificial Intelligence tools in financial institutions to improve the detection of complex laundering techniques, while maintaining human oversight to ensure compliance with the principles of legality and due process.
- 3.Encouraging wider participation of non-financial professions such as notaries, lawyers, and accountants in the reporting process, supported by awareness campaigns and simplified reporting mechanisms.
- 4.Amending and updating Algerian AML legislation (notably Law No. 05-01 and its amendments) to explicitly incorporate technological tools such as Artificial Intelligence and digital monitoring systems, while providing clearer provisions on

cyber security obligations for financial institutions and state authorities.

Bibliography List setting:

1. Legal and Constitutional References

- Algeria. Law No. 25-10 of 2025 on the Prevention of Money Laundering and the Financing of Terrorism.
- Algerian Law No. 09-04 of 16 August 2009 laying down specific rules relating to the prevention and fight against offences connected with information and communication technologies. Official Journal of the People's Democratic Republic of Algeria.
- Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering.
- Directive (EU) 2015/849 of 20 May 2015 (Fourth AMLD)
- Directive (EU) 2018/1673 of 23 October 2018 (Sixth AMLD)
- United Nations. (1988). Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances. Vienna.
- United Nations. (2000). Convention against Transnational Organized Crime (Palermo Convention). New York.
- United Nations. (2003). United Nations Convention against Corruption.

2. Academic References

- Chawki, M. (2015). Cybercrime, Digital Forensics and Jurisdiction. Springer.
- Daoud, M. M. (2022). A proposed framework for studying the impact of cyber security on accounting information to

increase trust in the financial reports in the context of industry 4.0: An event, impact and response approach. The Sixth Scientific Conference of the Faculty of Commerce, 42, 20-61. Syria: Tanta University.

- Emmanuel, A. A. (2025). The impact of cyber security on financial reporting: Strengthening data integrity. *International Journal of Science and Research Archive*, 2(14), 626-637.
- Molander, R. C., Mussington, D., & Wilson, P. A. (1998). *Cyber payments and Money Laundering: Problems and Promise*. RAND Corporation.
- Nour, B. A. (2022). The impact of ICT on the money laundering crime. *Critical Journal of Law and Political Science*, 17(1), 1048-1068.
- Opudu, D. O. (2024). Client confidentiality, data privacy and suspicious transactions reporting: the accountant's ethical dilemma in the Nigerian professional space. *UBS Journal of Business and Economic Policy*, 1(2), 109-121.
- Sorour, A. F. (2003). *Money Laundering and Terrorist Financing*. Cairo: Dar Al-Nahda Al-Arabiya.
- Wall, D. S. (2007). Policing cybercrimes: Situating the public police in networks of security within cyberspace. *Police Practice and Research*, 8(2), 187.
- Of Quebec, S., & Fortin, F. (2013). *Cybercrime: Between Misconduct and Organized Crime*. Presses inter Polytechnique.

3. Other / International Reports

- Financial Action Task Force (FATF). (2012). *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*. Retrieved June 13, 2025, www.fatf-gafi.org/recommendations.htm