

Money Laundering Using Modern

Dr. Khouas Nacera * Faculty of Law, University of Algiers 1, Comprehensive Development Mechanisms Laboratory in Algeria, Algeria, n.khouas@univ-alger.dz

Received: 28 /03/ 2026

Accepted:10 /05/ 2026

Published: 07 /06/ 2026

Abstract:

Modern technology has become a fundamental means of communication and information exchange today and in the near future. Society has shifted from a traditional model to a digital one, as technology has extended into all aspects of life, including financial transactions, which are increasingly carried out through digital spaces. This has opened the door to new forms of crime that differ from traditional crimes and are committed using technological tools—among them the crime of cyber money laundering, which has witnessed significant development, reflecting its seriousness and its threat to national economic security. The aim of this research paper is to identify the specific nature of cyber money laundering in terms of the methods used to commit it, its characteristics, and the mechanisms for combating it.

Keywords: money laundering, informatics, technology, electronic financial crime.

Jel Classification Codes: XN1, XN2.

الملخص

تعتبر التكنولوجيا الحديثة وسيلة أساسية للتواصل وتبادل المعلومات في الوقت الحالي وحتى في المستقبل القريب، إذ انتقلنا من مجتمع كلاسيكي إلى مجتمع رقمي، إذ امتدت التكنولوجيا إلى جميع مناحي الحياة، ومنها المعاملات المالية التي أصبحت تتم عبر الفضاءات الرقمية، ما فتح الباب إلى ظهور جرائم مغايرة للجرائم التقليدية تتم باستخدام الوسائط التكنولوجية منها جريمة تبييض الأموال المعلوماتية التي عرفت تطورا كبيرا ينم عن خطورتها على الأمن الاقتصادي الوطني. إن هدف هذه الورقة البحثية هو التعرف على خصوصية جريمة التبييض المعلوماتي من حيث أساليب ارتكابها، خصائصها وآليات مكافحتها. الكلمات المفتاحية: تبييض الأموال، المعلوماتية، التكنولوجيا، الجريمة المالية الإلكترونية.

* Corresponding author: Dr. Khouas Nacera,

INTRODUCTION

The world is witnessing a great development in modern technology, and its uses have expanded in several fields, including the field of business and banking, which has contributed to

improving the business and investment climate, and even contributing to facilitating banking and banking operations through the availability of electronic payment systems, digital banks, smart cash cards, and even electronic money... Etc. Under what is called artificial intelligence, banking operations have witnessed tremendous development, whether in terms of electronic money transfers, Internet banks, or statistics... Etc.

Despite the positives of this technological development, it had major and serious negatives, as new crimes emerged resulting from modern media and communication technology, most notably the crime of information money laundering, which benefited from this digital environment that motivated money launderers to legitimize criminal proceeds and gave them a greater opportunity and ease to commit this crime, this poses a real threat to all economic activities in the world and increases volatility in financial transactions, which has led to the closure of many banks, financial institutions and even commercial companies. Based on the above, we pose the following problem: How has modern technology contributed to the facilitation and transformation of money laundering practices, and what legal and institutional responses are required to effectively combat cyber/digital money laundering?

The importance of the research lies in the fact that cyber/digital money laundering constitutes a direct threat to the integrity and stability of national financial systems. It distorts legitimate markets, undermines public trust in banking institutions, and may facilitate the financing of organized crime networks and other illicit activities. Moreover, the borderless nature of digital infrastructures can weaken the effectiveness of purely domestic enforcement measures, thereby making technological capability, regulatory modernization, and international cooperation essential components of any credible anti-money laundering strategy. Accordingly, the study contributes to ongoing academic and policy debates by clarifying the conceptual specificity of digital money laundering and by linking technological modalities to legal and institutional countermeasures.

The objectives of the study are threefold. First, it aims to establish an academically precise understanding of cyber/digital money laundering by distinguishing it from traditional laundering while emphasizing its continuity in terms of core criminal purpose. Second, it seeks to identify and systematize the principal technological techniques and channels exploited by offenders, with attention to how these tools operate across the classical laundering stages (placement, layering, and integration). Third, it evaluates the Algerian legislative and institutional architecture for combating money laundering—particularly due diligence obligations, suspicious transaction reporting, financial intelligence mechanisms, and specialized judicial structures—in order to assess strengths, limitations, and possible areas for reform.

This study is divided into three main sections. Section I outlines the conceptual and legal foundations of cyber/digital money laundering, Section II examines the key technological techniques and digital channels that facilitate it, and Section III evaluates the Algerian legal and institutional response, concluding with targeted recommendations.

The first topic: The concept of information money laundering

The concept of information money laundering Money laundering is a new crime created by modern technologies. It falls under the category of economic crimes, which have maintained their

traditional character and been derived from cybercrime, making it a complex crime in terms of the techniques used to commit it, the difficulty of detecting it, and even the difficulty of defining a concept for it.

The first requirement: Definition of the crime of information money laundering

The term money laundering is one of the terms that appeared recently, after it began to be used in the United States of America (1920-1930) after World War I, indicating the criminal activities carried out by mafia gangs. The crime of money laundering has evolved from the traditional method to the modern method using technology.

Section One: Definition of traditional money laundering Money

Laundering is a complex crime that is based on several stages to give the legitimate character of dirty money that originally came from an illegal source (such as drug trafficking, terrorism crimes, illegal immigration and smuggling... etc). Money laundering means concealing the truth about money derived through an illicit route and showing it as if it were from legitimate sources or it can be described as transferring illicit money to economic systems.

Article 3(b)¹ of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances defines money laundering as: "the transfer or transfer of funds, knowing that they are derived from any crime or offenses set forth in subparagraph A of this paragraph [drug trafficking], or from an act of complicity in such crime or offenses." With the aim of concealing or camouflaging the illicit origin of the funds or with the intention of helping any person involved in committing such a crime or crimes to escape legal consequences². From the previous definitions, we conclude that the source of the crime of money laundering is an illegal source, especially with the growth of forms of crime, including:

- A. Illicit drug trafficking: Algeria is considered a transit area for this crime, which extends to Europe.
- b. The crime of terrorism and extremist groups
- C. Smuggling is one of the most common economic and financial crimes that Algeria suffers from.
- D. Illegal immigration, which has become an increasing activity of human trafficking networks, especially from the Sahel countries of Africa.
- E. Tax evasion, by not transparently declaring companies' business numbers and concealing real sources of transportation³.

The crime of money laundering is characterized by subjectivity, because it is carried out independently of the original crime regardless of whether the perpetrator of the original crime is convicted or not, and this is according to the text of Article 2 of Law No. 05-01 amended by Law 23/01, which was also amended by Law No. 25/10 of July 24, 2025, which includes the prevention and fight against money laundering and terrorist financing⁴.

Section Two: Definition of cybercrime and information money laundering

It was previously said that the crime of money laundering is one of the most serious economic crimes that has spread terribly, forcing countries to criminalize it under international

agreements, most notably the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances and the United Nations Convention against Organized Crime, but the danger has increased with the rapid technological development in the global economy, so we will try to define cybercrime and information money laundering.

First: Definition of cybercrime

There are many names for cybercrime, including "information crime", "cybercrime", "computer use crimes"... But the meaning is the same, and the jurist Don Parker, who uses the term "computer misuse," defined it as "any incident involving an intentional act that causes harm to the victim." Or he may suffer harm from it, and the perpetrator will receive a gain related to the misuse of computers. The Algerian legislator defined it in Article 2 of Law 09/04, which includes special rules for preventing and combating crimes related to information and communication technologies. It was called crimes related to information and communication technologies as: "crimes of tampering with automated data processing systems specified in the Penal Code and any other crime committed or facilitated by an information system or electronic communications system"⁵. Therefore, it can be said that modern technologies or the Internet allow traditional crimes to emerge and develop in the digital environment, providing them with modern methods that are easy, safer, and more complex at the same time.

Second: Definition of the crime of information money laundering

The crime of information money laundering is the result of a combination of the crime of traditional money laundering and cybercrime, as information and communication technology, especially the Internet, has provided a large space for this crime to be active, grow and spread, which has contributed to the complexity of mechanisms to combat it and limit its spread⁶. Therefore, if traditional money laundering is done by concealing the criminal origin from which the money comes, then information money laundering is "the use of modern technology or the Internet to camouflage the source of money and legitimize property that comes from criminal activities".

The process of information money laundering takes place in a complex manner, and includes three stages:

- 1- Deposit stage: This is the entry of funds obtained into the financial system using modern technology through electronic banks, electronic payment methods... Etc.
- 2- The concealment stage: It is done by separating dirty, illicit money from its illicit source by concealing it by following a series of financial operations that make it difficult to trace this money to reach its original source.
- 3- Merger: This process involves transferring illicit funds in a form that appears to everyone to be legal, such as purchasing real estate, investing in commercial projects, purchasing cars, and opening bank accounts in the name of family members.

The third requirement: Characteristics of the crime of information money laundering

The crime of information money laundering combines the crime of traditional money laundering with cybercrime. It is a modern financial crime that has spread through the spread of several technical means used by the perpetrators of the crime to camouflage the source of the money to make it appear legitimate, despite it retaining its traditional characteristics despite being committed using modern technological means, as it is considered one of the most dangerous economic crimes that affect the economic security of countries, it is also an original organized

crime with its connection to other crimes (terrorism, drug and human trafficking, smuggling, arms trafficking... etc).

1-Transnational crime: Money laundering takes information from cybercrime itself, exploiting the virtual world to commit it, making it cross-border (i.e., global). Cybercriminals use modern technology, whether computers, smart phones, or modern banking technologies, to make illegal or suspicious electronic money transfers from on.

2-soft and difficult-to-prove crime: This crime does not require force to commit it, but rather modern technological means. The impact of modern technology on the financial sector has been very great, as financial transactions, including transfers, payments, have become... Etc. It is done through digital means such as the Internet and mobile phones e country to another, especially with the availability of internet services. This directly affected the commission of the crime of money laundering for the cybercriminal, especially if he specializes in the field of informatics, as he cannot leave tangible physical evidence that facilitates the search and investigation process, which makes it a difficult crime to prove, requiring investigative officers specialized in cybercrimes to hide the trace of the cybercriminal to access Digital evidence⁷.

3-A new crime: Although money laundering is a traditional and ancient crime, with rapid technological development it has become an economic and financial crime with a new face through new means of committing it through the new means of committing it.

4- The crime of information money laundering is a soft crime: This crime is not committed with violence, but rather using technology and digital means in parallel with the digitization of the financial sector in general and the banking sector in particular, as financial transfers are now made via the Internet or smart phones, and using national and international bank accounts... Etc., all of this has made financial crime affected by cybercrime.

5-The crime of information money laundering is an economic and financial crime: The crime of information money laundering has taken technology as a means of committing it, so it is considered one of the new criminal forms with an economic dimension that transcends the borders of a single country, meaning that it crosses continents, as it is considered the product of illegal economic activities (such as drug trafficking, arms trade, illegal immigration, the crime of international terrorism...), the entry of this dirty money without knowing its source affects the stability of the national economy, causes it to lose balance, and makes it difficult for the state to confront and treat it, due to the entry of illicit money in large quantities, relying on methods of fraud and concealment⁸.

The second topic: Techniques and Digital Channels

Money launderers resort to using modern technology to commit this crime, whether by using modern banking technologies (the first requirement) or by using technologies over the Internet (the second requireme.

The first requirement: modern banking technologies

The financial and banking sector has developed like other sectors, especially with the development of technology accompanying globalization. Its financial services technologies have developed, and in parallel, criminals have worked to exploit this technological development to pass on their suspicious operations in the field of money laundering).

The crime of money laundering has moved from traditional methods to modern technological methods, which has made the work of judicial police officers and even investigators specializing in organized crime committed by digital means difficult. Through this requirement, we will attempt to highlight the most important electronic tools and methods used to commit this crime.

First: Internet banks

The Internet has led to the spread of e-commerce, and these banks are used to perform regular banking activities by opening accounts, transferring money, and paying bills... Etc.

Electronic banks or Internet banks also contribute to concluding some basic banking transactions without the presence of customers in the bank. This contradicts the principle of "know your business" stipulated in Article 7 of Law No. 05-01, as amended by Article 4 of Law No. 23-01 of February 6, 2023, relating to the prevention and combating of terrorist laundering and financing, which states: "Those subject to this must verify the identity of their customers, each with regard to him, when:

1-doing a business relationship.

2- Carrying out an incidental transaction that exceeds the ceiling specified by the organization, including in cases where the transaction is saved once or several times, and in which there appears to be a relationship between these operations.

3-Carrying out an incidental transaction in the form of an electronic payment that exceeds the ceiling specified by the regulation, or through several transactions that appear to be interconnected whose total exceeds this ceiling⁹.

4-The existence of suspicion of money laundering, financing terrorism, or financing the spread of weapons of mass destruction, separate from the ceiling set by the organization;

5-There is doubt about the validity or accuracy of the data related to the customer's knowledge that they previously obtained. Subjects must know the customer, whether he is permanent, occasional, natural or legal, and verify his identity through documents, data or information from reliable and independent sources. Information related to identity must be updated and the process of verifying this information must be carried out every year and every time it changes. This aforementioned article, before the amendment, did not discuss electronic payment as a modern means of money laundering, which allows banks and financial institutions to verify the identity of the customer or client, facilitating the process of tracking them in the event of suspicion of corruption or money laundering¹⁰.

Second: Electronic payment system E- payment systems

These systems are used in the process of depositing and withdrawing money from bank accounts. Article 6 of the Algerian E-Commerce Law defines it as "any payment method licensed in accordance with applicable legislation that enables its owner to make payments closely or remotely via an electronic system".

Electronic payment methods were initially introduced as a modern financial innovation aimed at simplifying transactions, enhancing efficiency, and facilitating the work of banks, financial institutions, and customers alike. These technologies were designed to promote financial inclusion, reduce reliance on cash, and accelerate the global transition toward digital economies. Through online banking, mobile payments, prepaid cards, and digital wallets, users gained unprecedented access to convenient and secure means of transferring money, paying bills, and managing accounts. However, as these systems became more widespread, they also introduced

new vulnerabilities within the financial sector. The anonymity, speed, and borderless nature of digital transactions have created opportunities for criminal actors to exploit these systems for illicit purposes, particularly in the field of money laundering. As a result, tools once intended to support legitimate economic activity have increasingly been manipulated to serve as conduits for concealing the origins of illegally obtained funds.

Money launderers exploit electronic payment platforms to convert illicit proceeds into seemingly legitimate digital funds by layering transfers across multiple accounts and instruments. This challenges detection at scale and requires enhanced due diligence, advanced transaction monitoring, and effective financial-intelligence coordination.

Third: Electronic money E-Money Electronic

Money is the most important tool used by money launderers. The idea of electronic money appeared in the 1990s under the obligation to reduce the use of cash, put it in digital form, and store it in a computer or smart card¹¹.

Electronic money can be defined as "cash value in the form of credit units stored electronically or on an electronic instrument held by the consumer". The customer purchases electronic currencies from the bank, which issues them and downloads them to the customer's computer. They are in the form of electronic units that replace regular currencies and have the same value. Electronic money is considered one of the most important tools for money laundering due to the impossibility of tracking it, its confidentiality, and its speed, through the deposit and merger stages, where any amount can be transferred in a short period without legal, geographical, or procedural obstacles¹².

Algeria has explicitly prohibited the issuance, purchase, sale, use, or possession of virtual assets under Law No. 25-10 (Article 6 bis, complementing Article 5 of Law No. 05-01), as a preventive response to the money-laundering risks associated with anonymity and traceability gaps in digital currencies. This prohibition reflects a risk-averse regulatory stance aimed at protecting financial stability, limiting illicit capital infiltration, and reinforcing compliance with AML/CFT obligations.

Fourth: Smart Cards

Card technology originated in England and spread to the United States of America. They are plastic One of the characteristics of these smart cards is that they can be programmed to store millions of dollars that can be transferred electronically to another card using a Smartphone without the intervention of any bank or financial institution. Thus, they are far from any monitoring, which facilitates the process of money launderers in transferring money from one country to another safely and using smart cards issued in one country to withdraw money in another country pieces that contain a chip (memory chip) to which the value can be encrypted. The smart card can also perform several roles at the same time (credit card, ATM withdrawal card, etc...) Which opens the door to the possibility of smuggling billions of dollars?

The second requirement: technologies used online

Criminal networks exploit online banking, digital payments, and e-commerce to move and disguise illicit funds quickly across borders. This fragmentation and layering reduces traceability and demands risk-based supervision, advanced transaction monitoring (including AI tools), and strong international cooperation.

First: e-commerce

The Internet has contributed to the emergence and spread of e-commerce

It can be defined as "an advanced form of trade characterized by the use of modern technology represented by the Internet in order to achieve the conclusion of contracts and deals effectively, quickly and with credit". Article 6 of the Electronic Commerce Law 18/05 defined it as "the activity whereby an electronic supplier proposes or ensures the provision of goods and services remotely to an electronic consumer, via electronic communications".

E-commerce is used as a means of committing the crime of money laundering by purchasing things that their owners offer via the Internet and social networking sites at prices that exceed their real price, with the aim of reselling them even if the profit margin is small, thus becoming a method of money laundering¹³.

Second: Selling an electronic public auction online

Modern technology has contributed to the spread of several activities and businesses. Even if an electronic contract is issued, it includes an electronic public auction contract, where the seller displays his goods to be sold after pricing them, and sets an opening price, and each bidder submits his offer at a higher price than the first until the final price is reached, and thus the auction is awarded to whoever p It should be noted that the E-Commerce Law of 2018 did not regulate these transactions, despite their regulation in the general rules of the Civil Code and the Algerian Civil and Administrative Procedures Law aid the most. Thus, the goods are supplied electronically or in a normal way to the beneficiary. Employing an electronic auction transaction over the Internet has become easy for money launderers, by paying huge sums of money and then integrating it into commercial transactions to become legitimate.

Third: Gambling via the Internet

Gambling has moved from real reality to virtual reality. If the Internet becomes an easy way for gambling companies to spread, they are used to launder money, especially if the laws of the country in question allow gambling online. A criminal who possesses money and illegal criminal proceeds employs gamblers and distributes illegal money to them. Money is laundered once these gamblers win, making it legitimate.

Online gambling is considered an illegal and unlawful activity in Algeria, according to Article 3 of Law No. 18-05 on Electronic Commerce, which states that "every transaction via electronic communications related to... is prohibited." Gambling, betting and lottery...".

The third topic: Criminalizing information Money laundering

Money laundering is widely recognized as one of the most persistent and adaptive forms of financial and economic crime. Traditionally, it has been understood as the process by which individuals or entities seek to disguise the illicit origin of funds derived from criminal activities, reintegrating them into the legitimate economy to obscure their unlawful source. While its fundamental nature remains constant, the crime has evolved significantly in both scope and sophistication. The rise of complex financial instruments, offshore accounts, and, more recently, digital currencies and online transactions has provided new avenues for concealing and transferring illicit proceeds. As these methods have grown more intricate, legislators and law enforcement authorities have had to respond dynamically, crafting updated legal frameworks capable of addressing the modern manifestations of this offense. Consequently, the phenomenon of information money laundering the use of information and communication technologies to

facilitate the laundering process—has emerged as a pressing concern that transcends national boundaries.

In response, states and international bodies have strengthened anti-money laundering frameworks through legislative reforms, specialized institutions (notably FIUs), and coordinated international standards and cooperation mechanisms (including FATF) to prevent, detect, and prosecute laundering in its evolving forms.

The first requirement: criminalizing information

Money laundering The Algerian legislator has criminalized money laundering in several laws, including general and specific laws. He stipulated the traditional crime of money laundering in Penal Code 04-1¹⁴ Articles 889 bis to Article 389 bis⁷. Article 389 bis stipulated that money laundering is considered:

- 1- Converting or transferring property with the perpetrator's knowledge that it is criminal proceeds for the purpose of concealing or camouflaging the illegal source of that property... Etc.
- 2- Hiding or disguising the true nature, sources or location of property... etc. The Algerian legislator has designated this crime with a special law due to the specificity of the means of committing it and its complexities, which is Law No. 05-01¹⁵ relating to the prevention of money laundering and terrorist financing and its status, amended and supplemented by Law No. 23-01 dated 2/7/2023.

It is noted that the Algerian legislator did not define the crime of money laundering, but rather limited the number of acts that constitute money laundering. Always within the framework of strengthening the legal system to prevent the crime of money laundering, Law No. 06/01 of 02/20/2006 was issued, which includes preventing and combating corruption, as it defined in Article 2 criminal proceeds as "all property derived and obtained directly or indirectly from committing the crime."

It also specified that an original crime is any crime from which proceeds come that could become the subject of money laundering. In the context of addressing new crimes and acts that affect automated data processing systems, Penal Code 04-15, which includes amending the Penal Code, includes a full section for this type of crime, which is Section 7 bis in Articles 394 bis to Article 394 bis 8, this was followed by a special text on crimes related to information and communication technologies, Law 09-04 of August 5, 2009, which includes special rules for the prevention of crimes related to information and communication technologies. This refers to electronic crimes or traditional crimes that take on a new face due to the use of modern technology in committing them, including the crime of information money laundering, especially with the absence of a special legal text to combat this new type of crime.

Article 16 of the Arab Convention on Combating Information Technology Crimes situates money laundering within the sphere of organized offenses facilitated by information and communication technologies. It emphasizes that digital environments can be used not only to execute illicit financial conduct but also to conceal its traces, thereby complicating detection, investigation, and prosecution. The provision extends criminalization beyond direct laundering to include assisting others in laundering and disseminating information, techniques, or methods

intended to enable such conduct. This approach reflects an expanded attribution of liability to those who knowingly support or facilitate laundering through technological means.

By framing laundering as an ICT-enabled crime, the Convention underscores the need for regional cooperation and the harmonization of legal standards among member states. It recognizes the borderless nature of cyberspace and calls for mutual legal assistance and structured information-sharing to address cross-jurisdictional laundering schemes. It also encourages strengthening national capacities in cyber forensics, financial intelligence, and digital surveillance to dismantle the technological infrastructure underpinning organized financial crime.

The second requirement: Mechanisms to combat the crime of information money laundering

The Algerian legislator has established institutional and judicial mechanisms to prevent the crime of information money laundering.

First: Let it process the financial inquiry

The Algerian legislator created the Financial Inquiry Processing Cell pursuant to Executive Decree No. 02-127 dated 04/07/2002, which includes the establishment of the Financial Inquiry Processing Cell and its organization, amended and supplemented by Executive Decree No. 08/275 dated 09/06/2008, amended and supplemented by Executive Decree 13/157 dated 04/15/2013.

The Financial Inquiry Processing Cell is an independent administrative authority that enjoys legal personality and financial independence, and exercises its powers under the supervision of the Minister of Finance. Executive Decree No. 22-36 dated 01/04/2022 defined the powers of the Financial Inquiry Processing Cell in accordance with Article 4 thereof, which stipulates that the cell is charged with combating money laundering and terrorist financing, and in this capacity it is charged with the following:

- Receiving statements of suspicion of terrorist financing and/or money laundering sent to it by bodies and persons designated by law (banks, financial institutions, non-financial institutions, liberal professionals, notaries, judicial bailiffs, public auction governors, lawyers. According to the aforementioned 2023 law and the previously mentioned 2025 law related to combating money laundering).
- Receiving and processing confidential reports and memoranda of the bodies stipulated in Article 21 of Law 05-01, as amended by Order 12-02.
- Reporting financial information to security and judicial authorities when there are methods to suspect money laundering or terrorist financing.
- Send, if necessary, the relevant file to the regionally competent public prosecutor.

Second: The National Committee for Assessing the Risks of Money Laundering, Financing Terrorism, and Financing the Proliferation of Weapons of Mass Destruction

Executive Decree No. 20-398 (26 December 2020) established a National Committee to institutionalize risk assessment for money laundering, terrorist financing, and proliferation financing. It reflects Algeria's shift toward a preventive, risk-based AML/CFT/CPF approach aligned with international standards and strengthened inter-institutional coordination. Under Executive Decree No. 20-398, the Committee functions as a national coordination and risk-assessment body that consolidates stakeholder input, produces and updates evidence-based national risk assessments, and translates their findings into policy and regulatory action to strengthen Algeria's preventive AML/CFT framework.

Article 4 of the aforementioned Executive Decree 20-398 specified the composition of this committee. As for its validity, it was determined by Article 2 of the same executive decree, and it can be summarized as follows:

- Study the sectoral reports and the national report on assessing the risks of money laundering, terrorist financing, and financing the proliferation of weapons of mass destruction and submit them for the approval of the Prime Minister.
- Propose any measure that would facilitate the conformity of national legislation and regulation with the recommendations issued by regional and / or international bodies to combat money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction.
- Accompanying the Financial Inquiry Cell in coordinating and following up on self- and mutual evaluation exercises for the national system to combat money laundering, terrorist financing, and financing the spread of weapons of mass destruction.
- Completing each study or initiative to develop useful mechanisms to identify and analyze money laundering methods. Financing terrorism and fina- Approval of the list of bodies subject to notification of suspicion.
- Proposing a list of countries with which information can be exchanged for approval by the Prime Minister, with an opinion on resorting to international technical assistance the spread of weapons of mass destruction.

Third: The National Committee for Operational Coordination

Overall, cyber/digital money laundering represents a technologically enabled evolution of a traditional offense that requires risk-based regulation, strengthened digital investigative capacity, and sustained inter-agency and cross-border cooperation.

Under Article 4 of Law No. 25-10 (24 July 2025), the Coordination Committee provides a unified framework that aligns Algeria's AML/CFT policies and operations with international standards by ensuring integrated action among regulators, law enforcement, and the judiciary. Beyond coordination, it supports risk evaluation, preventive design, and strengthened operational responses through sustained inter-agency communication, thereby enhancing the coherence and effectiveness of the national anti-money laundering system. The Coordination Committee is headed by the Head of the Financial Inquiry Processing Cell, and is formed, according to the text of Article 4 of the aforementioned Executive Decree 23-50, from members representing:

- Ministry of Interior, Local Authorities and Urban Planning,
- Ministry of Justice,
- National Gendarmerie Command,
- General Directorate of National Security
- Bank of Algeria,
- General Directorate of Customs, Official Gazette No. 2 issued on January 15, 2023.
- General Directorate of Taxes,
- General Directorate of National Property. The Coordination Committee shall carry out the tasks mentioned in Article 2 of the aforementioned Executive Decree, which can be summarized as follows:

- Contributing to the implementation of the national strategy to combat money laundering, terrorist financing.
- Ensuring coordination and exchange of operational information between the competent authorities with the aim of improving their effectiveness in combating money laundering, terrorist financing, and financing the spread of weapons of mass destruction.
- Requesting relevant information and data from the competent authorities in the field of combating money laundering and terrorist financing.
- Facilitating the exchange of information and statistics related to combating money laundering and terr-
- Taking all measures that allow for better cooperation between various actors in combating money laundering and terrorist financing.
- Taking all measures that allow for better cooperation between various actors in combating money laundering and terrorist financing. The Coordination Committee also prepares an annual report on its activities to be submitted to the Minister of Finance, in accordance with the text of Article 11 of the same Executive Decree.

Fourth: The jurisdiction of the economic and financial criminal pole to consider the crime of information laundering for money

Although the crime of information money laundering is a new crime due to the technological means by which it is committed, the Algerian legislator has referred jurisdiction to the economic and financial criminal pole due to its seriousness as an economic and financial crime without regard to the means of committing it.

Order 21-11 dated August 25, 2021, supplementing the Code of Criminal Procedure established by the National Criminal Pole for Combating Crimes Related to Information and Communication Technologies, did not stipulate the latter's jurisdiction to consider the crime of information money laundering. Rather, it explicitly stated that if the latter's jurisdiction and the economic and financial criminal pole combine, then preference belongs to the latter, according to the text of Article 211 bis 28 of Order 21/11.

The Economic and Financial Penal Pole was established pursuant to Law No. 20-04 amending the Code of Criminal Procedure, to combat economic and financial crimes, in accordance with Article 211 bis of Order 20. 04 The above-mentioned statement states: "A specialized national criminal pole will be established at the level of the Court of the Reporters of the Council of Algiers to combat economic and financial crime."

Article 211 bis 2 of Order 20-04 exclusively defines crimes that are complex and fall within the scope of the jurisdiction of the Criminal and Financial Pole, namely:

- Crimes stipulated in Articles 119 bis, 389 bis, 389 bis 1, bis 2 and bis 3 of the Penal Code (which is the crime of money laundering).
- Crimes stipulated in Law 06-01 dated 02/20/2006 related to preventing and combating corruption.
- Crimes stipulated in Order 96-22 of July 9, 1996, relating to the suppression of violations of legislation and regulations relating to exchange and capital movement.
- The crimes stipulated in Articles 11, 12, 13, 14 and 15 of Order 05/06 of August 23, 2005 relating to combating smuggling."

Article 211 bis 3 of Order No. 20-04 assigns jurisdiction to the Criminal and Financial Division when money laundering is committed through information and communication technologies, reflecting the legislator's recognition of the heightened technical sophistication of

digital-era financial crime. By classifying ICT-enabled laundering among the most complex economic and financial offenses, the provision confirms that such cases require specialized judicial expertise, operational coordination, and technological competence to ensure effective investigation, prosecution, and adjudication.

Under this framework, a “complex economic and financial crime” includes offenses whose scope, organization, or impact makes them difficult to investigate and adjudicate—due to multiple actors, wide geographic reach, serious harm, or an organized and transnational character. The use of ICT further increases complexity by requiring specialized investigative techniques, digital forensics, and, where cross-border transactions are involved, enhanced international judicial cooperation, thereby justifying specialized jurisdiction under Article 211 bis 3.

CONCLUSION

The crime of money laundering using modern technology (information money laundering) is a new traditional crime, produced by media and communication technologies, which has given it the peculiarities of electronic crime, especially in the stage of investigation, investigation, and search for digital evidence. Through this study, we have reached a set of results that can be summarized as follows:

- The crime of information money laundering, a crime independent of the original crimes for which the source of the money is illicit (tax evasion, illegal immigration, human trafficking, smuggling, terrorist financing, arms trafficking...etc.).
- Through Law 23-01, the Algerian legislator expanded the list of those subject to the Money Laundering Prevention Law to include, in addition to financial institutions, non-financial institutions and professions.

The Algerian legislator has established institutional and judicial mechanisms to prevent and combat the crime of information money laundering, the most important of which are the Financial Inquiry Cell, the National Committee for Assessing the Risks of Money Laundering, Terrorist Financing, and Financing the Proliferation of Weapons of Mass Destruction, all the way to the newly created Coordination Committee under Law 23-01 and Law 25 – 10, In addition, the Economic and Financial Criminal Pole was established to consider the crime of information money laundering as an economic and financial crime, even if it was committed using information and communication technologies. According to the text of Article 211 bis 2 of Law 20-04, dated 2020 supplementing the Code of Criminal Procedure, jurisdiction devolves to the Economic and Financial Criminal Pole.

Suggestions that can be made include the following: It is recommended to attach research, investigation and inquiry into information money laundering crimes to the National Criminal Pole for crimes related to information and communication technologies, given the specificity of the advanced technological means used in committing the crime. The necessity of modernizing the banking system, with the establishment of digital platforms for customers to carry out financial operations.

Bibliography List:

- Algeria, (2002), Executive Decree No. 02-127 of 07 April 2002 establishing and organizing the Financial Inquiry Processing Cell, amended and supplemented by

Executive Decree No. 08-275 of 06 September 2008 and Executive Decree No. 13-157 of 15 April 2013, Algeria.

- Algeria, (2004), Law No. 04-15 (2004) containing the Penal Code, Official Gazette, No. 71, Algeria.
- Algeria, (2005), Law No. 05-01 of 06 February 2005 relating to the prevention and combating of money laundering and terrorist financing, Official Gazette, No. 08, Algeria.
- Algeria, (2006), Law No. 06-01 of 20 February 2006 on the prevention and combating of corruption, Official Gazette, No. 14, supplemented by Order No. 10-05 of 26 August 2010, and amended and supplemented by Law No. 11-15 of 02 August 2011, Algeria.
- Algeria, (2009), Law No. 09-04 of 05 August 2009 containing special rules for the prevention and combating of crimes related to information and communication technologies, Official Gazette, No. 47 (issued 16 August 2009), Algeria.
- Algeria, (2018), Law No. 18-05 of 10 May 2018 relating to electronic commerce, Official Gazette, No. 28 (issued 16 May 2018), Algeria.
- Algeria, (2020), Executive Decree No. 20-398 of 26 December 2020 establishing the National Committee for Assessing the Risks of Money Laundering, Terrorist Financing, and the Financing of the Proliferation of Weapons of Mass Destruction, Official Gazette, No. 80 (issued 29 December 2020), Algeria.
- Algeria, (2020), Law No. 20-04 of 30 August 2020 amending and supplementing the Code of Criminal Procedure and establishing the economic and financial criminal pole, Official Gazette, No. 51 (dated 31 August 2020), Algeria.
- Algeria, (2021), Order No. 21-11 of 25 August 2021 supplementing the Code of Criminal Procedure relating to the National Criminal Pole for Combating Crimes Related to Information and Communication Technologies, Algeria.
- Algeria, (2022), Executive Decree No. 22-36 of 04 January 2022 specifying the tasks and powers of the Financial Inquiry Processing Cell, its organization and operation, Official Gazette, No. 03 (issued 09 January 2022), Algeria.
- Algeria, (2023), Executive Decree No. 23-50 of 03 January 2023 establishing an operational committee to coordinate policies and operations to combat money laundering and terrorist financing and defining its tasks, organization and functioning, Official Gazette, No. 02 (issued 15 January 2023), Algeria.
- Algeria, (2023), Law No. 23-01 of 07 February 2023 amending and supplementing Law No. 05-01 relating to the prevention and combating of money laundering and terrorist financing, Official Gazette, No. 08 (issued 08 February 2023), Algeria.
- Algeria, (2025), Law No. 25-10 of 24 July 2025 relating to the prevention and combating of money laundering and terrorist financing, Official Gazette, No. 48, Algeria.
- League of Arab States, (2010), Arab Convention to Combat Information Technology Crimes, Cairo, 21 December 2010 (ratified by Algeria in 2014), Arab Region.

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

—

Citations:

- 1- The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988.
- 2- The Arab Convention to Combat Information Technology Crimes issued on December 21, 2010, which Algeria ratified pursuant to Presidential Decree

2014.dically. The necessity of training judges in cybercrime and how to use modern technology.

3- Law No. 05-01 of February 6, 2005 relating to preventing and combating money laundering and terrorist financing, No. 08.

4- Law No. 04/15 of 2004 containing the Penal Code, c.R, number 71.

5- Law 06/01/ dated 02/20/2006 containing the prevention and combating of corruption, c. R, No. 14, supplemented by Order No. 10-05 dated 8/26/2010, amended and supplemented by Law 11-15 dated 08/02/2011.

6- Law 09/04 of August 5, 2009, containing special rules for the prevention and control of crimes related to information and communication technologies, c. R, Issue 47, issued on August 16, 2009.

7- Law No. 18/05 of May 10, 2018 relating to electronic commerce c. R, Issue 28, issued on May 16, 2018.

8- Law 23/01 of February 7, 2023 amending and supplementing Law No. 05/01 relating to the prevention and combating of money laundering and terrorist financing, c. R, Issue 8, issued on February 8, 2023.

9- Law No. 25/10 of July 24, 2025 relating to the prevention and combating of money laundering and terrorist financing, Official Gazette No. 48.

10- Law No. 20/04 of August 30, 2020 amending and supplementing the Code of Criminal Procedure, including the financial economic pole, c. R, No. 51, dated 08/31/2020.

11- Order 21-11 of August 25, 2021 supplementing the Code of Criminal Procedure relating to the National Criminal Pole for Combating Crimes Related to Information and Communication Technologies.

12- Executive Decree 02/127 dated 04/07/2002 establishing and organizing the Financial Inquiry Processing Cell, amended and supplemented by Executive Decree No. 08-275 dated 09/06/2008, amended and supplemented by Executive Decree 13/157 dated 04/15/2013.

13- Executive Decree No. 20- 398 dated 12/26/2020, including the establishment of committees The National Committee for Assessing the Risks of Money Laundering, Financing Terrorism, and Financing the Proliferation of Weapons of Mass Destruction, Official Gazette, No. 80, issued on 12/29/2020.

14- Executive Decree No. 22/36 dated 01/04/2022 specifying the tasks and powers of the Financial Inquiry Processing Cell, its organization and operation, Official Gazette No. 3 issued on January 9, 2022.

15- Executive Decree 23/50 of January 3, 2023 establishing an operational committee to coordinate policies and operations to combat money laundering and terrorist financing and to define its tasks, organization and conduct, Official Gazette No. 2 issued on January 15, 2023.

