

Legal Mechanism for the Prevention and Control of Money Laundering through Electronic Communication Networks under Algerian Business Law

Azeddine Mebrek ¹, and Zakia Djedaini ²

¹ Doctor, University of Yahia Fares in Media, Faculty of Law, Algeria

Email: mebrek7@gmail.com

² Professor, University of Algiers1, Ben Youssef Ben Khada, Faculty of Law, Algeria.

Email: zakiadjedaini49@gmail.com

Abstract---Money laundering, whether committed through traditional methods or more prominently via modern technological means, has become one of the fastest-growing and most widely spread crimes globally, particularly over the past two decades. This alarming expansion has drawn the attention of states and both governmental and non-governmental organizations, especially those that have entered into international and regional agreements aimed at its prevention and control. As a transnational and organized crime, money laundering has prompted the Algerian legislator to take proactive measures to criminalize and sanction it, in accordance with the provisions of relevant international conventions. In this regard, Algeria has established specialized national bodies and institutions dedicated to the prevention and suppression of this economic and financial crime. On another front, perpetrators of this crime have not remained confined to conventional methods of execution. Instead, they have adapted to the scientific and technological advancements of the modern era, utilizing information and communication technologies (ICTs) and the internet as effective tools to launder illicit and dirty funds, thereby giving them a semblance of legitimacy. Consequently, money laundering is now carried out through sophisticated techniques across electronic communication networks in various forms and dimensions. These platforms offer speed and ease of execution while posing significant challenges to the collection of evidence and the prosecution of offenders.

How to Cite:

Mebrek, A., & Djedaini, Z. (2025). Legal mechanism for the prevention and control of money laundering through electronic communication networks under Algerian Business Law. *The International Tax Journal*, 52(5), 2488–2502. Retrieved from <https://internationaltaxjournal.online/index.php/itj/article/view/259>

The International tax journal ISSN: 0097-7314 E-ISSN: 3066-2370 © 2025

ITJ is open access and licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

Submitted: 11 January 2025 | Revised: 19 March 2025 | Accepted: 12 July 2025

2488

Keywords---Money laundering crime, electronic communication networks, electronic banking transactions, Financial Intelligence Processing Unit, electronic payment methods.

Introduction

Money laundering is widely recognized as one of the gravest financial and economic crimes confronting the contemporary global order, owing to its deeply disruptive impact on national economic systems. It functions as a structural nexus that underpins all forms of unlawful economic activity and the illicit proceeds generated therefrom, posing a persistent threat to the integrity and stability of legitimate financial frameworks.

The primary objective pursued by perpetrators of this crime is to confer a veneer of legitimacy upon funds originating from criminal sources. This is achieved by channeling such illicit assets into the formal financial sector, particularly through banks and financial institutions, in order to conceal their unlawful origins and enable their integration and investment into economic ventures. These ventures may outwardly appear to be legitimate development projects, yet in reality, they serve as conduits for laundering illicit capital.

Due to the seriousness of this crime, which has become the focus of attention of many countries, and which have concluded many international and regional agreements to prevent and combat it, as it is an organized and cross-border crime, it has become a real challenge to banks and financial institutions of the governments of countries, which strive to prevent and combat it.

Algeria is not immune from the latter, especially after the scientific and technological development that the world is witnessing in the current era, which was a catalyst for the introduction of the element of technology and the need to establish information networks for information and communication in all fields and sectors, including commercial transactions and the settlement of the payment system. have serious effects on the economies and financial systems of countries, due to the perpetrators benefiting from this scientific and technological development and harnessing it to commit many financial and business crimes through the electronic network, including the crime of money laundering.

In order to prevent and combat this economic and financial crime, the Algerian State has ratified some conventions related to this criminal phenomenon, including the Vienna Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of December 20, 1980¹. It also ratified the Arab Convention on Combating Money Laundering and the Financing of Terrorism, signed in Cairo on 21 December 2010.²

In this context, and in affirmation of the necessity to activate preventive measures against the crime of money laundering, the Algerian legislator has enacted a comprehensive arsenal of legal provisions. The most prominent among them include the following:

Ordinance No. 96-22 on the suppression of violations of legislation and regulation relating to the exchange and movement of capital to and from abroad³, and Law No. 05-01 on the prevention and

1- Algeria has ratified with reservation the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, concluded in Vienna on 20 December 1988, by Presidential Decree No. 95-41 of 28 January 1995, G.R. No. 07 of 15 February 1995.

2- Algeria ratified the Arab Convention against Money Laundering and the Financing of Terrorism, adopted in Cairo on 21 December 2010, by Presidential Decree No. 14-250 of 08 December 2014, G.R. No. 55 of 23 December 2014.

3- Ordinance No. 96-22 of July 9, 1996, on the suppression of violations of legislation and regulation relating to exchange and movement of capital to and from abroad, G.R. No. 37 of 15 June 2003.

combating of money laundering and the financing of terrorism⁴, as well as Law No. 09-04, which contains the rules on the prevention and combating of crimes related to information and communication technologies⁵. Based on the above, we can raise the following problem:

Are the mechanisms enshrined within the Algerian legal system sufficient and effective to prevent and combat the crime of money laundering through the electronic communications network?

This study is structured into two main sections: the first outlines the conceptual framework of money laundering through electronic communication networks, while the second examines the preventive mechanisms established within the Algerian legal system to combat this crime.

Chapter One: The Conceptual Framework of the Crime of Money Laundering through the Electronic Communications Network

Due to the scientific and technological development that our world is witnessing in the current era, it has become possible to launder money remotely, by connecting to the electronic network, and in order to clarify this in detail, we have dedicated the first requirement to the definition of the crime of money laundering using the electronic communication network, and the second requirement To study the characteristics of the crime of laundering using the electronic communication network.

First Requirement: Definition of Money Laundering Crime Using the Electronic Telecommunications Network

In this demand, we try to define the crime of money laundering through the electronic telecommunications network (**Section-one**), and then address the characteristics of this financial and economic crime of an electronic nature (**Section-two**).

Section One: Definition of the Crime of Money Laundering through the Electronic Telecommunications Network

Before addressing the definition of the crime of money laundering committed through the electronic network, we must first address the definition of this crime in its traditional guise, and then address the definition of the electronic network of communications and highlight how the crime of money laundering is committed through its technical and technical means.

First: Legal Definition of Money Laundering Crime

We can define the crime of money laundering according to what is stated in international conventions first and then define it according to what is stated in Algerian legislation

1. **Definition of money laundering crime in international conventions:** The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances defines the crime of money laundering as: "**the process of transferring, transferring, concealing or disguising the truth of money.**"⁶ It also stipulates that: "**Acquisition, possession or use of funds knowing at the time of receipt that they are the result of the crime of illicit drug trafficking.**"⁷

The United Nations Convention against Transnational Organized Crime (**Palermo Convention**) of 2000 also defined it in its Article VI (06) as:

a) "**Transfer or transfer property, knowing that it is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of such property, and assisting any person**

⁴- Law N°. 05-01 of 06 February 2005 on the prevention and combating of money laundering and the financing of terrorism, G.R. No. 11 of 09 February 2005, as amended and supplemented.

⁵- Law No. 09-04 of 25 August 2009 on the Prevention and Combating of Crimes Related to Information and Communication Technologies, G.R. No. 47 of 16 August 2009.

⁶- See article 03, paragraph 02/b, of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988.

⁷- See article 03, paragraph 01/c, *ibid*.

- involved in the commission of the original offence from which it came, in order to escape actual legal penalties."
- b) "Concealing or disguising the true nature, source, location, manner of disposal, movement, ownership, source or rights related thereto, knowing that they are the proceeds of crime."
 - c) "Acquisition, possession or use of property knowing at the time that it is the proceeds of crime."
 - d) "Participating in the commission of any of the offences stipulated in this article, collusion or conspiracy to commit them, attempting to commit them, assisting, inciting, facilitating or advising in respect thereof."

A close examination of these definitions reveals that the Palermo Convention has significantly broadened the scope of illicit and dirty funds by adopting a comprehensive definition that encompasses various sources of criminal activity. This stands in contrast to the Vienna Convention, which confines the origin of illicit funds exclusively to drug-related offenses.

1. Definition of the crime of money laundering in Algerian legislation

Referring to national legislation, article 389 of Law No. 04-15⁸ defines the crime of money laundering as follows: "Money laundering shall be considered as follows:

- Any transfer or transfer of funds with the knowledge that the actor is the direct or indirect proceeds of a crime for the purpose of concealing or disguising the illicit source of such funds or assisting any person involved in the commission of the original crime from which such funds were obtained to escape the legal consequences of his acts.
- Concealing or disguising the true legal nature, source, location, manner of disposal, movement, or rights related to the funds, knowing that they are the proceeds of crime.
- Acquiring or using funds with the person doing so knowing at the time of receipt that they constitute criminal proceeds.
- Participation in the commission of any of the offences prescribed in accordance with this article, or collusion, conspiracy to commit or attempt to commit them, assisting, inciting, facilitating, and advising thereon."

This definition is the same as the one provided by the legislator in the text of Article 02 of Law 05-01⁹, on the prevention and combating of money laundering and the financing of terrorism, with a slight change, as it included the term money instead of the term property in the body of the article.

It is also evident that the definitions adopted by the Algerian legislator have broadened the scope of illicit or "dirty" funds to include all criminal proceeds, regardless of the nature of the predicate offense. Moreover, the legislator has enumerated various forms of participation and complicity in the crime, in addition to those outlined in Article 42 of the Algerian Penal Code.

Second: Jurisprudential Definition of Money Laundering Crime

A recognized strand of English legal scholarship defines money laundering as follows: "knowingly transferring, depositing, or transferring funds obtained from an illegal activity, or assisting in such operations with the intention of concealing the truth of such funds, and this crime includes cases in which the ownership of suspicious funds is acquired, possessed or used, knowing at the time that they are the result of a crime or participation in it."¹⁰

Egyptian legal doctrine also defines this crime as: "**all the procedures followed to change the character of the funds, and then obtain them by illegal means, to appear as if they originated from a legitimate source.**"¹¹

⁸- Law No. 04-15 of 10 November 2004, G.R. No. 71 of 10 November 2004, amending and supplementing Ordinance No. 66-156 of 08 June 1966 containing the Penal Code.

⁹- See the text of article 02 of Law No. 05-01, op. cit.

¹⁰- Nader Shafi Abdel Aziz, *The Crime of Money Laundering, A Comparative Study*, Modern Book Foundation, Lebanon, 2005, p. 34.

¹¹- Fouad Shaker, *Money Laundering and its Impact on the National Economy*, Lectures in Banking Studies, Central Bank, Egypt, 1996, p. 54.

Accordingly, we conclude from these definitions that the crime of money laundering is the process of concealing the illicit sources of movable and immovable funds, resulting from the commission of organized crimes, such as drug trafficking, financing of terrorism, arms smuggling, counterfeiting of money, trafficking in human beings, and embezzlement of funds, in order to clean them up and legitimize them by including them within the scope of the economic cycle. By listing them in investment and commercial projects and trading them legally.

Third: Definition of the Electronic Telecommunications Network

The electronic telecommunication network is defined as a set of electronic devices and means connected to each other, thus forming a complex global web that connects the entities of societies and institutions in countries, using smart means and technologies for digital communication with interconnection as well as randomness, such as computers, smartphones, routers, servers, optical fibers transmitting data, and telecommunication stations Digital platforms that work through the exchange of electromagnetic waves and satellites that transmit data between them across the globe¹².

In other words, it is a wide range of electronic devices that include computers and smartphones, which are connected to each other by electronic devices, cables, and optical fibers dedicated to telecommunications, distributed throughout the world, and these electronic devices store a huge amount of **big data**, so that it is accessed by connecting it to the Internet, by an Internet distribution device called a modem **and its own** Internet **address (IP)**, where it is obtained by Internet Service Providers (FAI).¹³

Thus, with this scientific and technological development in the field of information and communication, the electronic network has pushed the world to a great qualitative progress in transactions between various people and entities and in various fields, especially commercial transactions, which have moved from the time of traditional commerce to the era of electronic commerce and a new era called the digital age.

Section Two: Characteristics of the Crime of Money Laundering through the Electronic Telecommunications Network

The crime of money laundering committed through the electronic telecommunications network is characterized by many characteristics and characteristics, the most important of which can be mentioned as follows:

First: The crime of money laundering is a financial and economic crime

The crime of money laundering is a purely financial and economic crime, as it affects the state's economy and financial system, which threatens its entity with collapse, because money derived from dirty and illegal sources, which are integrated into the state's economy to the point of legitimizing it, does not play any positive role in supporting economic development, but quickly returns badly as soon as it is withdrawn from banks after acquiring the status of legitimacy¹⁴.

Second: The crime of money laundering is a subsidiary crime

The crime of money laundering is considered a subsidiary crime par excellence, as it is assumed that it arises as a result of the occurrence of an original crime that preceded it, and is therefore a source of dirty money, resulting from criminal activity or an illegal source of money, where it was collected

¹²- Simon Cooley, *Online Commerce*, International House of Ideas, Amman, 1999, p. 15.

¹³- Issa Lafi Hussein Al-Samadi, *The Legal Responsibility of Electronic Banking in Jordanian Legislation*, Electronic Financial Transfer, Ph.D. Thesis in Private Law, Faculty of Law, University of Algiers, 1, 2010, p. 27.

¹⁴- Nadia Abdel Rahim, *Anti-Money Laundering in the Algerian Banking System*, Ph.D. Thesis, Faculty of Economics, Commercial Sciences and Management Sciences, University of Algiers 3, 2014, p. 215.

directly or indirectly as a result of the offender committing crimes punishable by law¹⁵. For its part, the Algerian legislature has expanded the concept and scope of predicate offences, provided that they are also considered to be predicate offences by foreign law, in accordance with the provisions of article 389 bis of the Algerian Penal Code and article 02 of Law No. 05-01, as amended and supplemented.

Third: The crime of money laundering is an organized crime

The crime of money laundering is committed in deliberate and deliberate ways by organized persons or entities, which have their own rules and regulations, and work in complete secrecy in order to obtain quick financial profit, regardless of the nature of its sources, and for this purpose a number of economists, law and public relations experts are recruited to defend it against any judicial prosecution whatsoever¹⁶.

Fourth: The crime of money laundering is an international crime

The information revolution in the field of digital communications has contributed to a great extent to exacerbating the phenomenon of money laundering and its crossing of the borders of a single country, as commercial transactions and electronic transfers of money have become carried out through the Internet, in open and cross-border digital spaces, so that it has become the dominant feature in commercial and financial practices of an electronic nature¹⁷. This led to money whistleblowers benefiting from these technological advantages and transferring dirty and illegal money from one country to another, in order to legitimize it and remove it from all suspicions¹⁸.

Second Requirement: Reasons for Committing the Crime of Money Laundering Using the Electronic Telecommunications Network

Modern communication technology has brought about radical changes in the lives of individuals and institutions, so that it has produced new concepts, perhaps the most important of which are e-commerce, electronic commercial contracts, electronic and digital banks and financial institutions, digital blockchains, electronic payment and transfer of money, and other electronic transactions that are among the reasons that directly help in committing The crime of money laundering in the electronic environment.

Section One: E-commerce as a Means of Money Laundering

E-commerce has been able to make a quantum leap in economic development, and has been able to achieve the public benefit that benefits individuals, companies, and society alike, but it has been the cause of the spread of the crime of money laundering and a means of employing it.

First: Definition of E-commerce

The World Trade Organization (OMC) defines e-commerce as: "**the production, sale and distribution of products through telecommunication networks.**"¹⁹ The Asia-Pacific Economic Cooperation (APEC) also defined it as: "**any form of commercial transactions and services in which the parties deal electronically, whether between a person and another person, between a person and a computer, whether between businesses and consumers, or between each of them separately and between government departments.**"²⁰

¹⁵- Khaloufi Khadouja, Lonnie Farida, The Elements of the Crime of Money Laundering in Algerian Legislation, Article published on www.asjp.cerist.dz website, accessed 15/12/2022, at 21:30, pp. 604-605.

¹⁶- Fadia Qassem Beydoun, From the Crimes of White-Collared Owners, Bribery and Money Laundering, Al-Halabi Human Rights Publications, First Edition, Lebanon, 2008, p. 21.

¹⁷- Tariq Kazim Ajil, The Crime of Money Laundering, a Study of Its Nature and the Penalties Prescribed for It, an article published in the Journal of Integrity and Transparency for Research and Studies, Iraq, First Issue, 2009, p. 41.

¹⁸- Alia Laschab, The Legal Framework for Anti-Money Laundering, Diwan of University Publications, Algeria, 2007, pp. 26-29.

¹⁹- Nidal Ismail Ibrahim, Provisions of E-Commerce Contracts, Dar Al-Farqa for Publishing and Distribution, First Edition, 2005, p. 15.

²⁰- Mohamed Al-Serafi, Electronic Management, Dar Al-Fikr Al-Jami'a, First Edition, Cairo, 2006, p. 158.

Referring to the Algerian legislature, electronic commerce is defined under article 06 of Law 18-05 as: **"the activity whereby an electronic supplier proposes or guarantees the remote provision of goods and services to an electronic consumer, through electronic communications."**²¹

As for jurisprudence, some jurists in the law have defined it as: **"the project's presentation of products and services on Internet sites, for the purpose of obtaining requests from customers."**²² Some others defined it as: **"all commercial transactions, including the purchase, sale, and exchange of products, services, information, financial settlement, and banking transactions, using electronic means."**²³

Second: Using e-commerce as a means of committing the crime of money laundering

²⁴ The crime of money laundering goes through three main stages, namely the deposit stage, the employment stage, and the integration stage, where e-commerce is resorted to in the second stage of the money laundering crime, i.e. dirty money is employed to legitimize it, before integrating it into economic projects. dirty finances, and camouflage their commercial nature, in order to avoid knowing their source and source by the agencies concerned with monitoring them.

Therefore, this stage is considered one of the most dangerous and difficult stages, thanks to which the stage of integrating the capacity funds into economic projects is reached, and thus it is legitimized in a way that ultimately seems legal, which leads to the difficulty of proving its original²⁵ guilt.

In this context, it can be concluded that e-commerce represents one of the most effective means by which money launderers are able to bypass two critical stages of this organized criminal enterprise: the placement of illicit funds into commercial activities, and the final integration of those funds into legitimate economic projects that serve as a safe haven for them.

Section Two: Electronic Banks as a Means of Committing the Crime of Money Laundering

Electronic banking distinguishes itself by offering services that surpass those of traditional banks, catering more effectively to customer needs—particularly in light of ongoing developments in commercial and financial sectors, such as e-commerce and electronic payment and fund transfer systems. These platforms enable banks to reach a broader client base, deliver high-quality financial services, reduce operational costs, and enhance performance efficiency. However, these advantages have not prevented money launderers from exploiting such banking technologies to carry out their illicit activities.

First: Definition of Electronic Banks

E-banks are an important pillar of banking operations and remittances, which meet the needs of customers according to the pattern imposed by the Information and Communication Technology (TIC) revolution, which has had a strong impact on various vital fields, including the financial and banking field, of which electronic banking is one of the most important pillars.

The term e-banking is used to refer to the financial services that banks benefit from remotely, and electronic banks are defined as: **"those banks and financial institutions, which rely on electronic media to keep pace with developments in the field of information and communication technology, and to provide all banking services securely and with less cost, in the fastest time"**

²¹- Law No. 18-05 of 10 May 2018 on e-commerce, G.R. No. 28 of 16 May 2018.

²²- Wassima Mustafa Hanshour, *The Legal System of E-Commerce in Algerian and Comparative Legislation*, Ph.D. Thesis, Faculty of Law and Political Science, Abdelhamid Ben Badis University, Mostaganem, 2017, p. 38.

²³- Mohamed Saeed Ahmed Ismail, *Methods of Legal Protection for E-Commerce Transactions, A Comparative Study*, Al-Halabi Human Rights Publications, Lebanon, 2016, p. 38.

²⁴- Abdel Fattah Bayoumi Hijazi, *The Crime of Money Laundering through the Internet, An In-depth Study on the Crime of Money Laundering through Electronic Media in Comparative Legislation*, Dar Al-Nahda Al-Arabiya, Egypt, 01st Edition, 2009, p. 18.

²⁵- Law No. 06-01 of 20 February 2006 on the prevention and combating of corruption, G.R. No. 14 of 8 March 2006.

and with the least effort for customers, such as computers, ATMs, internet, and others."²⁶ It is also defined as: "All banks and financial institutions that provide their banking services to their customers, through an information communication network, thus providing the principle of security, low costs, and profiting time."²⁷

Referring to the Algerian legislator, he did not define electronic banks in the Money and Loan Law or in any other relevant laws or regulations issued by the Bank of Algeria²⁸, but with reference to Law No. 06-01 on the prevention and combating of corruption, he used the phrase "**banks that do not have a physical presence and are not attributed to a regulated financial group**" It is a metaphor for electronic banks, as recently addressed in Law No. 23-09 on the Monetary and Banking Law²⁹, the terms digital banks and the digital dinar as a direct reference to the orientation of the legal and economic system in Algeria towards this digital transformation in the monetary and banking system.

Based on the aforementioned definitions, it can be stated that electronic banking represents the most effective model for expressing digital banking and financial transfers. This system relies on the internet and other electronic platforms to deliver services remotely, without requiring the physical presence of clients. Such an approach facilitates faster banking operations, electronic payments, and fund transfers, while simultaneously reducing time, effort, and operational costs.

Second: The Use of Electronic Banks in the Crime of Money Laundering

The emergence of e-commerce has resulted in the idea of electronic payment, which is carried out through electronic media connected to the Internet, which is an important part of electronic banking based on electronic banking, and is closely related to e-commerce, thanks to which money can be transferred electronically from one account to another³⁰. This process is carried out By means of electronic payment cards or credit cards, as defined by the legislator under Article 543 bis 23 of the Commercial Code as follows: "**A payment card shall be considered any card issued by banks and financial bodies that are legally qualified and allow its holder to withdraw or transfer funds...**". However, these cards may be used in illegal ways, such as in the crime of money laundering, in fraudulent ways, such as:

- Using an expired bankcard to purchase goods or obtain services equivalent to the value of the illicit money returned to the bank when it is returned.
- The use of a cancelled bank card, it may happen that the bank or financial institution issuing the card cancels it during its validity due to its misuse by the cardholder, but nevertheless the holder concludes transactions for the purchase of goods or services, and pays for the same with such cancelled card, and upon its reversal by the card issuer. It pays its dues from illegal funds with the aim of laundering it³¹.
- Money laundering can also be done through the electronic money transfer technology, where criminals use this technology to transfer their dirty money in order to clean it abroad, as this process guarantees them the required speed and confidentiality while transferring money to and from abroad. In this case, the perpetrators deposit their money with banks to be transferred directly to the accounts of shell companies located abroad.

²⁶- Al-Abdullat, Abdel Fattah Zuhair, Obstacles to the Expansion of the Use of Electronic Banks, Case Study of Banks Operating in Yemen, Journal of Social Studies, University of Science and Technology, Issue 30, 2010, p. 69.

²⁷- Jalila Abdel Jalil, Ben Abdel Fattah Dahman, Electronic Banking, its Services and Risks, Revue des réformes électroniques et intégration en économie mondiale, Volume 13, Issue 01, 2019, p. 254.

²⁸- Salih Bounkla, The Legal System of Electronic Banking Operations, Ph.D. Thesis, Faculty of Law and Political Science, University of 08 May 1945, Guelma, 2020, p. 80.

²⁹- Law No. 23-09, of 21 June 2023, incorporating the Monetary and Banking Code, Official Gazette of the Republic of Algeria, No. 21, of 08 April 2020.

³⁰- Ibrahim Al-Desouki AbuAl-Lail, Legal Aspects through Modern Means of Communication, Research Presented at the Conference on Law, Computers and the Internet, College of Sharia and Law, United Arab Emirates University, 2000, p. 05.

³¹- Abdel Fattah Bayoumi Hijazi, op. cit., pp. 54-55.

Chapter Two: Mechanisms for Preventing the Crime of Money Laundering through the Electronic Network

The twentieth century produced an unprecedented revolution in the field of information and communication technology, which contributed to the promotion of human life in various economic, social and cultural fields, but on the other hand, it had its negative impact represented in the illegal use of these technologies, which led to the assault on the legally protected interests of persons and institutions, through the commission of many cybercrimes. Among which is the crime of laundering money through the electronic network.

In this context, the Algerian state has sought to take cognizance of this economic crime by working to establish specialized bodies in the prevention and combating of this crime, taking into account the specificity of the means used in its implementation, which is represented in the electronic network, and among the most important of these bodies is the Financial Information Processing Cell (**the first requirement**), and the National Authority for the Prevention of Crimes Related to Information and Communication Technologies (**Second Requirement**).

First Requirement: Financial Query Processing Cell

The crime of money laundering through electronic networks is one of the complex economic crimes, due to the scientific and technological progress that coincided with economic globalization, which in turn contributed to the creation of organized and cross-border criminal gangs, which necessitated the development of legal mechanisms to protect and protect public funds from this crime, which is becoming more and more sophisticated and complex day by day Executive No. 13-157³². However, before addressing the role of this cell in the prevention of money laundering, it is necessary to present the legal framework of this body and define its competencies.

Section One: Legal Framework of the Financial Inquiry Processing Cell

This cell is one of the bodies created at the national level to implement the international obligations agreed upon within the framework of activating the role of banks and financial institutions, to detect money laundering operations in all its forms and means, which lead to harm and harm of public funds, especially in light of the technological developments taking place in the electronic environment of financial and banking activities at the national and international levels.

In this context, and following Algeria's ratification of the Convention on Cooperation against Organized Crime,³³ the Algerian legislature issued Executive Decree No. 02-127, which includes the establishment, organization and functioning of this cell.

First: The Legal Nature of the Automated Inquiry Processing Cell

According to the provisions of Executive Decree No. 02-127, the Cell enjoys legal personality and financial independence, as Article 2 of the Cell includes the definition of the Financial Inquiry Processing Cell as: "**a public institution enjoying legal personality and financial independence...**"³⁴, but this definition raises the problem of the lack of independence of this cell and its subordination to the Minister in charge of Finance, as the legislator stipulates that it "**shall be placed with the Minister in charge of Finance...**".

- As a result, the unit becomes institutionally subordinate to the executive authority, represented by the Minister of Finance, thereby lacking the power to independently appoint its personnel or organize its internal affairs. This situation contradicts the notion of financial autonomy attributed to the unit, revealing the limited scope of its independence. In addition to this structural constraint, several other limitations further restrict the unit's autonomy, among which the most notable are:

³² - See Executive Decree No. 02-127 of 07 April 2002, establishing the Financial Inquiry Processing Unit, as amended and supplemented by Executive Decree No. 13-157 of 15 April 2013, G.R. No. 23 of 28 April 2013.

³³ - See document A/RES/55/25 of the United Nations Convention against Transnational Organized Crime, adopted and submitted for signature, ratification and accession by United Nations General Assembly resolution 25, fifty-fifth session, of 15 November 2000.

³⁴- See the text of article 02 of Executive Decree No. 02-127, op. cit.

- The cell does not have its own financial budget, as it is subject to funding from the public treasury to manage its affairs.
- The power to appoint its president and members shall be monopolized by the President of the Republic, and on the proposal of the Minister in charge of Finance.

Second: Composition of the Cell

In accordance with the text of Article 04 of Executive Decree No. 08-275,³⁵ amending and supplementing Executive Decree No. 02-127, the composition of the Council of the Financial Inquiry Processing Cell shall consist of the following:

- President
- Secretary General of the Cell,
- Four judges to be selected based on their competence in the banking and financial field,
- Two judges appointed by the Minister of Justice, Hafez Al-Khatam, after taking the opinion of the Supreme Judicial Council.

Third: Administrative Departments of the Financial Inquiry Processing Cell

The Cell is assisted in the performance of its tasks by four technical departments, which were established and organized by a joint ministerial decision dated May 28, 2007, issued by the Minister of Finance, the Secretary-General of the Government and the Director General of the Public Service.³⁶

1. **Investigations and Investigations Department:** This department is tasked with gathering information, analyzing suspicious statements, conducting the necessary investigations to control suspicious operations, and receiving notifications of suspicion received.
2. **Legal Department:** It is responsible for the legal affairs and relations with the Public Prosecution of the competent judicial authorities, and it is also responsible for studying the legal aspects of the files and reports submitted before it, in order to analyze their facts and ensure that they conform to the elements of the crime.
3. **Documents and Database Department:** This department is tasked with collecting and preserving documents and information related to financial operations by documenting all the data collected in its own database, for the sake of the proper functioning of the Cell.
4. **The Department of Cooperation:** It is entrusted with bilateral and multilateral relations between the Cell and the national and foreign bodies that work with it in the same field, due to the specificity of the crime of money laundering as a regular crime with an international dimension, as its investigations require the Cell to inquire, investigate and investigate inside and outside the borders of the State.

Section Two: Competencies of the Financial Inquiry Processing Cell

The Financial Intelligence Processing Unit (FIF) at the national and international levels undertakes the following tasks:

- Receive Suspicious Notifications
- Analyze and Manipulate Notifications
- Investigate suspicious financial transactions and receive suspicious notices about them.
- According to the text of Article 04 of Executive Decree 06-05 of 09/01/2006, notifications of suspicion mean: " **Any transaction of any nature: financial, banking, selling, buying, transfers...**", which raises suspicions as to whether they were made with dirty and illegal funds, obtained from the crime of money laundering, the financing of terrorism, or otherwise.
- According to the text of Article 19 of Law 05-01, as amended and supplemented, the following persons are subject to the duty to notify the suspect:
- Banks, Financial and Banking Institutions

³⁵- See the content of Executive Decree No. 08-275 of 06 September 2008, amending and supplementing Executive Decree No. 02-127 of 07 April 2002, establishing the Financial Intelligence Cell, its organization and functioning.No. 50, of 07 September 2008.

³⁶- See the Joint Ministerial Decision dated 28 May 2007 regulating the technical interests of the Financial Inquiry Processing Cell, issued in the Official Gazette No. 30 of 13 June 2007, p. 27.

- Financial interests of Algeria Post and other similar financial institutions
- Insurance Companies & Exchange Offices
- Cooperatives, Bets & Casinos

1. Any natural or legal person who, within the framework of his duties, consults or conducts deposits, transfers, exchanges, employments or any other movement of capital, especially at the level of liberal professions in various forms, especially including :lawyers, notarization, auction portfolios, accounting experts, bookkeepers, brokers and customs agents, brokers and brokers in the stock exchange process, real estate agents, billing institutions, dealers of precious stones and precious metals, dealers of antiquities and artifacts, tax and insurance authorities, directorates of real estate The state, the public treasury, and others³⁷.

In this regard, it is imperative that the aforementioned individuals and entities promptly notify the financial intelligence unit by submitting confidential reports as soon as they suspect that any transaction or deal may be linked to money laundering activities even if such operations appear legitimate and sound on the surface .

As observed above, the Algerian legislator has granted both natural and legal persons broad authority to report suspected cases of money laundering to the Financial Intelligence Unit (FIU), which has been vested with full powers to investigate and examine such reports. This reflects the legislator's intent to tighten control over offenders who seek to launder criminal proceeds through various means in order to give them a veneer of legitimacy. It is worth noting, however, that the FIU is not authorized to initiate investigations on its own initiative; nonetheless, it plays a vital role in preventing the commission of money laundering offenses, particularly those carried out via electronic networks.

Second Requirement: National Authority for the Prevention of ICT-Related Crimes

The crime of money laundering committed through the electronic network is considered one of the cross-border information crimes, which is considered the most complex due to the multiplicity of perpetrators and the multiplicity of those affected by it, due to the expansion of the crime scene as well as the difficulty of arresting the perpetrators and proving their crime. Responsible for the prevention of crimes related to information and communication technologies, which was established in order to implement the international obligations agreed upon in the framework of combating cybercrime, especially the crime of money laundering through the Internet.

Although Algeria delayed the establishment of this body due to the political and security conditions it was experiencing at the end of the last century, it followed the example of many countries that it created to reduce criminal phenomena of an electronic nature, most notably the crime of money laundering through the electronic network. We devoted the first section to the study of its legal framework, and the second section was devoted to defining its competencies.

Section One: Legal framework of the National Authority for the Prevention of Crimes Related to Information and Communication Technologies

Article 13 of Law No. 09-04 stipulates that: **"A national commission shall be established for the prevention and combating of crimes related to information and communication technologies, which shall determine the composition, organization and manner of its conduct through regulation"**, and³⁸ in 2019 Presidential Decree No. 19-172 was issued, which includes the composition, organization and functioning of the commission.³⁹

³⁷ - See the text of article 19 of Law No. 05-01 of February 6, 2005, on the prevention and combating of money laundering and the financing of terrorism, as amended and supplemented, Official Gazette No. 11 of February 9, 2005.

³⁸- Law No. 09-04 of 05 August 2009 on the Special Rules for the Prevention and Combating of Crimes Related to Information and Communication Technologies, G.R. No. 47 of 16 August 2009.

³⁹- See Article 01 of Presidential Decree No. 19-172 of 06 June 2019, which specifies the composition of the National Authority for the Prevention, Combating and Regulation of Crimes Related to Information and Communication Technologies, and how it operates, IRG 37, of 09 June 2019.

First: The Legal Nature of the National Authority for the Prevention of Crimes Related to Information and Communication Technologies

According to the text of Article 02 of Presidential Decree No. 19-172: "The Authority is a public institution of an administrative nature, with legal personality and financial independence, placed at the disposal of the Ministry of National Defense", and enjoys the independence that enables it to perform the tasks entrusted to it to the fullest, but the latter is not absolute, as it is subject to an authority above it, represented by the Ministry of National Defense.

Second: Composition of the National Authority for the Prevention of Crime and Information and Communication Technologies

According to article 04 of Decree No. 19-172, the National Authority for the Prevention of Crimes Related to Information and Communication Technologies is composed of two administrative bodies that assist it in the performance of its mandated tasks, namely a Steering Council and a General Directorate, where:

1. **Steering Council:** Chaired by the Minister of National Defence or his representative, it consists of the Ministry of National Defence, the Ministry in charge of the Interior, the Ministry of Justice, and the Ministry in charge of Telecommunications.
2. **General Directorate:** Managed by the Director General, and includes the Technical Directorate and the Directorate of Administration and Means.

Section Two: Terms of Reference of the National Authority for the Prevention of Crimes Related to Information and Communication Technologies

Presidential Decree No. 19-172 specifies the composition of the National Authority for the Prevention of Crimes Related to Information and Communication Technologies, which is composed of the aforementioned Steering Council and the General Directorate, who are entrusted with a set of competencies, which we summarize below:⁴⁰

First: Competencies of the Steering Council

The Steering Council deliberates on the National Strategy for the Prevention and Combating of ICT-Related Crimes, as well as issues of development and cooperation with national institutions and bodies concerned with this type of crime.

It also periodically assesses situations that pose a threat in relation to ICT-related crimes through monitoring and taking note of them in order to achieve the precise objectives pursued, in addition:

- Each research and evaluation activity proposes direct work in this field and approves the Authority's work program.
- Prepares and certifies its Rules of Procedure.
- Examines and approves the annual reports of the Authority's activities and budget.
- It expresses its opinion on the annual reports of the Authority's activities, makes suggestions thereon, and sets the legal standards that fall within its area of competence.

Second: Competencies of the General Directorate

The Directorate-General, as an administrative organ of the National Authority for the Prevention of Crimes Related to Information and Communication Technologies, exercises the following functions:

- Ensuring the proper functioning of the Authority, preparing its draft budget and implementing its work programs.
- Activate and coordinate the prevention of technology-related crimes and communication in cooperation with the Steering Board.
- Exchange of information with foreign counterparts for the purpose of collecting data on perpetrators and locating them.

⁴⁰- See the content of Articles 04, 05, 06, and 09 of Presidential Decree No. 19-172, previous source.

- Preparing and preparing the meetings of the Steering Council.
- Prepare the annual report related to the activities of the National Authority.
- The Technical Directorate has also been entrusted with the task of preventive monitoring of electronic communications within the framework of the prevention of crimes described as terrorist acts and attacks on State security, and it also works to assist the judiciary and the judicial police services at their request.
- Collecting, recording, locating and tracking digital data for use in judicial proceedings⁴¹.

Conclusion

In conclusion, and in light of the foregoing, it can be asserted that money laundering through electronic communication networks constitutes a form of contemporary crime that transcends national borders and remains difficult to monitor and control. This complexity is further exacerbated by rapid advancements across various fields, particularly the widespread use of technological tools and artificial intelligence systems, which have come to dominate most economic, commercial, and financial activities. These developments have given rise to a range of criminal phenomena that threaten the very fabric of states and societies, targeting public order and undermining economic and financial stability.

In pursuit of curbing this criminal phenomenon, the Algerian legislator has, since 2004, introduced a series of legal mechanisms and technical measures aimed at preventing and containing money laundering in a manner that aligns with the evolving nature of the crime itself. These efforts have been complemented by the establishment of specialized administrative, security, and judicial bodies tasked with combating this category of offenses, which continue to grow in complexity in tandem with the rapid expansion and sophistication of the digital environment.

Despite the array of legal instruments and technical measures dedicated to curbing money laundering through electronic networks in Algeria, the fight against this crime remains challenging. This difficulty stems primarily from the lack of adequate technical infrastructure capable of effectively monitoring the flow of funds from origin to destination, investigating their sources, and prosecuting those responsible. For these reasons, among others, it can be concluded that preventing and containing this form of organized economic crime requires the concerted efforts of security, legal, social, and technological sectors to achieve the desired objectives. Accordingly, the following recommendations are proposed as part of the concluding section of this research paper:

First: The need to develop an information system at the level of banks and financial institutions, which should be locally established, in order to avoid breaches of information systems and the personal and professional data of customers, especially since most of the information gaps come from outside the borders of the state, which aim to compromise the security and economic stability of the state.

Second: Modernization and modernization of the legal system in line with the developments in various fields, especially in the commercial and financial field, which is experiencing rapid development, which has resulted in a remarkable development of the crime of money laundering.

Third: Concluding regional and international cooperation agreements between banks and financial institutions to develop the legal, security and technical system to prevent the crime of money laundering by modern technological means.

Fourth: According to the wire system for financial transfers, many banks are not members of the **Fedwire system**, and only a few of them are members of the **Chips** system or what is known as:

⁴¹- See the content of Articles 11 and 09 of Presidential Decree No. 19-172, *ibid*.

international system House Clearing, which results in money laundering by fraudulent means. All banks should make public the use of the **Swift** system, which monitors the movement of funds across bank accounts, and requires prior declaration of the source of the funds to be transferred before the transaction can be carried out.

Fifth: Granting the Financial Information Processing Cell and the National Authority for the Prevention of Crimes Related to Information and Communication Technologies full powers to perform their tasks to the fullest, and placing all material and human means at their disposal without referring to other bodies in order to approve the implementation of the tasks entrusted to them, especially since the two bodies are active in vital fields.

Sources & References

First: List of Sources

1. United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, concluded in Vienna on 20 December 1988, ratified by Algeria by Presidential Decree No. 95-41 of 28 January 1995, Official Gazette of the Republic of Algeria No. 07, dated 15 February 1995.
2. The Arab Convention against Money Laundering and the Financing of Terrorism, drafted in Cairo on 21 December 2010, ratified by Algeria by Presidential Decree No. 14-250 of 08 December 2014, Official Gazette of the Republic of Algeria No. 55, of 23 December 2014.
3. Decree No. 96-22 of July 9, 1996, on the suppression of violations of the legislation and regulation of exchange and movement of capital to and from abroad, Official Gazette of the Republic of Algeria No. 37 of 15 June 2003.
4. Law No. 05-01 of 06 February 2005 on the prevention and combating of money laundering and the financing of terrorism, Official Gazette No. 11 of 09 February 2005, as amended and supplemented.
5. Law No. 06-01 of 20 February 2006 on the prevention and combating of corruption, Official Gazette of the Republic of Algeria n° 14, of 08 March 2006.
6. Law No. 06-23 amending and supplementing Decree No. 66-156 containing the Penal Code, of 20 December 2006, Official Gazette of the Republic of Algeria No. 84, of 24 December 2006.
7. Law No. 09-04 of 05 August 2009, containing the Rules on the Prevention and Combating of Crimes Related to Information and Communication Technology, Official Gazette of the Republic of Algeria No. 47, of 16 August 2009.
8. Law No. 18-05, of 10 May 2018, on electronic commerce, Official Gazette of the Republic of Algeria n° 28, of 16 May 2018.
9. Law No. 23-09, of 21 June 2023, incorporating the Monetary and Banking Code, Official Gazette of the Republic of Algeria, No. 21, of 08 April 2020.
10. Presidential Decree No. 19-172 of 06 June 2019 establishing the composition of the National Authority for the Prevention, Combating and Regulation of Crimes Related to Information and Communication Technologies, Official Gazette of the Republic of Algeria No. 37, of 09 June 2019.
11. Executive Decree No. 02-127 of 07 April 2002 establishing the Financial Intelligence Processing Unit, as amended and supplemented by Executive Decree No. 13-157 of 15 April 2013, Official Gazette of the Republic of Algeria No. 23 of 28 April 2013.
12. Executive Decree No. 08-275 of 06 September 2008 amending and supplementing Executive Decree No. 02-127 of 07 April 2002 establishing the Financial Information Cell (FIS) and its functioning, Official Gazette No. 50 of 07 September 2008.

Second: References Bibliography

Books:

1. Nader Shafi Abdel Aziz, The Crime of Money Laundering, A Comparative Study, Modern Book Foundation, Lebanon, 2005.

2. Fouad Shaker, Money Laundering and its Impact on the National Economy, Lectures in Banking Studies, Central Bank of Egypt, 1996.
3. Fadia Qassem Beydoun, White-Collar Crimes, Bribery and Money Laundering, Al-Halabi Human Rights Publications, Edition 01, Lebanon, 2008.
4. Alia Laschab, The Legal Framework for Anti-Money Laundering, Diwan of University Publications, Algeria, 2007.
5. Mohamed Ahmed Ismail, Methods of Legal Protection for E-Commerce Transactions, A Comparative Study, Al-Halabi Human Rights Publications, Lebanon, 2016.
6. Abdel Fattah Bayoumi Hegazy, The Crime of Money Laundering Through the Internet, An In-Depth Study on the Crime of Money Laundering through Electronic Media in Comparative Legislation, Dar Al-Nahda Al-Arabiya, Egypt, 01st Edition, 2009.
7. Ibrahim El-Desouki AbuAl-Lail, Legal Aspects through Modern Means of Communication, Research Presented at the Conference on Law, Computer and the Internet, College of Sharia and Law, United Arab Emirates University, 2000.

Academic Theses

1. Issa Lafi Hussein Al-Samadi, The Legal Responsibility of Electronic Banking in Jordanian Legislation, Electronic Financial Transfer, Ph.D. Thesis in Private Law, Faculty of Law, University of Algiers 1, 2010.
2. Nadia Abdel Rahim, Anti-Money Laundering in the Algerian Banking System, Ph.D. Thesis, Faculty of Economics, Commercial Sciences and Management Sciences, University of Algiers 3, 2014.
3. Salih Bounkla, The Legal System of Electronic Banking Operations, Ph.D. Thesis, Faculty of Law and Political Science, University of 08 May 1945, Guelma , 2020.

Academic Article

1. Khaloufi Khadouja, Loni Farida, The Elements of the Crime of Money Laundering in Algerian Legislation, an electronic article published on the www.asjp.cerist.dz website, accessed 15/12/2022, at 21:30.
2. Al-Abdullat, Abdel Fattah Zuhair, An Article on the Obstacles to the Expansion of the Use of Electronic Banks, A Case Study of Banks Operating in Yemen, Journal of Social Studies, University of Science and Technology, Issue 30, 2010.
3. Jalila Abdel Jalil, Ben Abdel Fattah Dahman , Electronic Banking, its Services and Risks, **Revue des réformes électroniques et intégration en économie mondiale**, Issue 01, 2019.