

Dirassat & Abhath
The Arabic Journal of Human
and Social Sciences



مجلة دراسات وأبحاث
المجلة العربية في العلوم الإنسانية
والاجتماعية

EISSN: 2253-0363
ISSN : 1112-9751

**Combating electronic money laundering through international cooperation:
Study in the framework of international law**

مكافحة تبييض الأموال الإلكترونية من خلال التعاون الدولي: دراسة في ضوء القانون الدولي

Pr. ZAADI Mohamed Djelloul

University of Bouira, Faculty of law and political sciences, Department of public law,
m.zaadi@univ-bouira.dz

أ.د. زعادي محمد جلول

جامعة البويرة، كلية الحقوق والعلوم السياسية، قسم القانون العام

m.zaadi@univ-bouira.dz

تاريخ النشر: 2026/10/15

تاريخ القبول: 2026/09/19

تاريخ الاستلام: 2026/06/20

Abstract:

The rapid expansion of digital financial services, electronic payment systems, and virtual assets has significantly transformed the global financial landscape, while simultaneously creating new opportunities for criminals to engage in sophisticated electronic money laundering activities. Owing to the transnational nature of these crimes, individual states often encounter substantial legal, technical, and jurisdictional challenges in their efforts to detect, investigate, and prosecute offenders. This study examines the role of international cooperation in combating electronic money laundering within the framework of international law by analyzing the legal mechanisms, institutional arrangements, and collaborative measures adopted at the international level. Particular attention is devoted to the contribution of international conventions, mutual legal assistance, information exchange mechanisms, extradition procedures, and the standards established by the Financial Action Task Force. The study further explores the effectiveness of cooperation among national financial intelligence units, law enforcement agencies, and judicial authorities in addressing emerging laundering techniques associated with cryptocurrencies, online banking, and cross-border electronic transactions.

Keywords: Electronic money laundering; International cooperation; International law; Mutual legal assistance; Information exchange; Transnational financial crimes.

المخلص:

أدى التطور المتسارع للخدمات المالية الرقمية، وأنظمة الدفع الإلكتروني، والأصول الافتراضية إلى إحداث تحولات جوهرية في النظام المالي العالمي، كما أتاح في الوقت ذاته فرصاً جديدة لمرتكبي الجرائم المالية لممارسة عمليات تبييض الأموال الإلكتروني بوسائل أكثر تعقيداً وخفاءً. ونظراً للطبيعة العابرة للحدود لهذه الجرائم، تواجه الدول تحديات قانونية وتقنية وقضائية متعددة تعيق جهودها الرامية إلى الكشف عن مرتكبيها وملاحقتهم ومعاقبتهم. تهدف هذه الدراسة إلى بحث دور التعاون الدولي في مكافحة تبييض الأموال الإلكتروني في إطار القانون الدولي، من خلال تحليل الآليات القانونية والترتيبات المؤسسية والتدابير التعاونية المعتمدة على الصعيد الدولي. وتركز الدراسة على إسهامات الاتفاقيات الدولية، والمساعدة القانونية المتبادلة، وآليات تبادل المعلومات، وإجراءات تسليم المجرمين، والمعايير الصادرة عن فرقة العمل المعنية بالإجراءات المالية لمكافحة غسل الأموال وتمويل الإرهاب. كما تتناول مدى فعالية التعاون بين وحدات الاستعلام المالي الوطنية، وأجهزة إنفاذ القانون، والسلطات القضائية في مواجهة الأساليب المستحدثة لتبييض الأموال المرتبطة بالعملة المشفرة، والخدمات المصرفية الإلكترونية، والتحويلات المالية العابرة للحدود.

الكلمات المفتاحية: تبييض الأموال الإلكتروني؛ التعاون الدولي؛ القانون الدولي؛ المساعدة القانونية المتبادلة؛ تبادل المعلومات؛ الجرائم المالية العابرة للحدود.

1.Introduction:

The contemporary world is witnessing rapid developments in digital technology and electronic communications, leading to the emergence of new forms of transnational financial crime, most notably electronic money laundering, which has become a real challenge for both national and international legal systems. With the significant expansion in the use of digital media, electronic banking services, virtual currencies, and electronic payment

platforms, the transfer of funds and the concealment of their illicit sources have become more complex and faster, granting criminal groups extensive opportunities to exploit the digital space to funnel their illegal proceeds beyond the reach of traditional financial institutions.

Electronic money laundering is a modern extension of traditional money laundering, distinguished by its use of electronic means and modern technologies at all stages, whether related to depositing,

concealing, or integrating funds. This allows for the concealment of the illicit origin of funds derived from various predicate offenses, such as drug trafficking, corruption, cybercrime, human trafficking, and terrorist financing. Furthermore, the virtual nature of these transactions makes it difficult to trace the flow of funds or identify those involved, especially given the multiplicity of jurisdictions and the differences in legal systems between countries.

In this context, the urgent need for international law intervention has emerged to establish a comprehensive legal framework to address this growing phenomenon. This framework should include rules for international cooperation, information exchange, and the strengthening of financial and digital oversight mechanisms. This has been embodied through numerous international and regional treaties and conventions that have sought to criminalize money laundering and strengthen the obligations of states in the field of prevention, detection and judicial prosecution, most notably the United Nations Convention against Transnational Organized Crime, and the Financial Action Task Force, which established international standards for combating money laundering and terrorist financing, as well as the efforts made within the framework of the United Nations and Interpol to promote international security and judicial cooperation.

Despite the multitude of international legal mechanisms, combating cyber money laundering continues to face several practical and legal challenges. These include the transnational nature of these crimes, the increasing use of encryption technologies and cryptocurrencies, weak coordination among national regulatory systems, and the challenges associated with proving cybercrime and determining the criminal liability of individuals and entities involved. Furthermore, the issue of balancing the fight against financial crime with ensuring the protection of digital privacy and the free

flow of data is a significant challenge. This necessitates a continuous review and adaptation of traditional legal instruments to technological advancements.

Therefore, studying the fight against cyber money laundering in international law is of paramount importance, given its close connection to protecting the global economy, ensuring the integrity of financial systems, and enhancing international security and stability. This study also aims to analyze the effectiveness of existing international legal mechanisms for addressing this crime, assess their capacity to keep pace with rapid digital transformations, and identify the most prominent legal and institutional challenges hindering an effective international response in this area.

The Importance of the Research:

The importance of studying the topic of combating electronic money laundering in international law lies in its relevance to contemporary legal issues driven by rapid digital transformations and the increasing reliance on modern technology in financial and commercial transactions. Electronic money laundering crimes have become a direct threat to the stability of economic and financial systems, given the ease with which electronic means can conceal the sources of illicit funds and transfer them across borders without physical or effective oversight. This necessitates examining international legal mechanisms capable of addressing this phenomenon.

The study's importance is further highlighted by its close connection to protecting national and international economies from illicit financial flows that negatively impact the investment climate and contribute to the spread of corruption, organized crime, and the financing of illegal activities, including terrorism and cybercrime. Successful efforts to combat electronic money laundering will enhance confidence in digital financial institutions and ensure the integrity of electronic transactions within the global digital economy.

The study's significance is further highlighted by its emphasis on the role of international law in establishing a cooperative legal framework among states to address the transnational nature of this crime. This framework is developed through international agreements and recommendations issued by the Financial Action Task Force, as well as by promoting judicial and security cooperation and information exchange between countries. The study also contributes to assessing the effectiveness of these legal mechanisms in keeping pace with modern technological advancements, particularly with the proliferation of digital currencies and electronic payment platforms.

Furthermore, the study holds both academic and practical importance. It enriches legal research related to financial cybercrime and helps provide legal insights and recommendations that can support national and international legislative policies aimed at closing legal gaps and enhancing the effectiveness of anti-money laundering systems in the evolving digital environment.

Research Objectives:

This study of combating electronic money laundering in international law aims to shed light on the conceptual and legal framework of this emerging crime. It will clarify the concept of electronic money laundering, its characteristics, and its most prominent forms and modern methods related to the use of digital technology and electronic media to conceal and legitimize illicit proceeds.

The study also seeks to analyze the various international legal mechanisms adopted to combat electronic money laundering. This will be achieved by examining the most important relevant international and regional treaties and conventions, as well as the role of the Financial Action Task Force in setting international standards and recommendations to combat money laundering and terrorist financing in the digital environment. Furthermore, the study will assess the effectiveness of international

judicial and security cooperation in tracing and recovering illicit funds.

The study also aims to highlight the legal and technical challenges facing international efforts to combat electronic money laundering, particularly those related to the transnational nature of this crime, the difficulty of tracing digital financial transactions, the use of cryptocurrencies and modern encryption technologies, and the challenge of reconciling the requirements of combating money laundering with respect for digital privacy and the protection of personal data.

Furthermore, the study seeks to assess the adequacy and effectiveness of current international legal frameworks in addressing this crime, identifying shortcomings or gaps that may limit their effective implementation. This will allow for the proposal of legal solutions and recommendations that can enhance international cooperation and develop the legislative and regulatory framework to address the growing risks of electronic money laundering in light of rapid digital development.

The problematic:

Based on the above, it logically follows that we ask the following problematic:

To what extent has the conceptual framework of the crime of electronic money laundering and the mechanisms of international cooperation contributed to the development of an effective legal system to combat this crime and reduce its challenges in light of technological development and its transnational nature?

Research Structure:

This study is divided into two complementary sections. The **first section** addresses the conceptual framework of electronic money laundering, while the **second section** examines the mechanisms for combating electronic money laundering under international law.

Scientific Methodology:

Given the complex nature of electronic money laundering, its study necessitated a multidimensional methodological approach combining legal, technical, and analytical methodologies. This approach allows for a comprehensive understanding of the phenomenon within its digital and legal context. In this regard, the descriptive-analytical method was adopted as the primary methodology for this study. This method allows for a description of the phenomenon as it exists in the digital world, an analysis of its characteristics and methods of implementation, and an exploration of the contexts in which it is prevalent. The study focuses on the electronic stages involved in money laundering operations, such as digital transfers, cryptocurrency wallets, transactions via decentralized platforms, and methods of anonymization.

The comparative method was also employed when examining the legal framework, both nationally and internationally. This involved comparing legislation related to combating traditional and electronic money laundering and analyzing the differences in strategies adopted by various legal systems. This approach allows us to highlight strengths and weaknesses, and to draw lessons from the experiences of countries that have developed advanced regulatory systems to deal with digital financial crimes.

2. The Conceptual Framework of Electronic Money Laundering:

Electronic money laundering is one of the most prominent challenges facing financial and legal systems in the modern world, given the significant development of digital technologies and the widespread use of the internet in financial transactions. Electronic money laundering is generally defined as the process by which funds obtained from illegal activities are transformed into seemingly legitimate funds using electronic means and digital technologies, making it more difficult for regulatory bodies and legal authorities to trace their original source.

This type of crime reflects the transformation of traditional money laundering into a digital phenomenon, where criminals exploit the speed, anonymity, and openness to cross-border markets offered by modern technologies such as e-banks, cryptocurrencies, digital wallets, and online trading platforms. The conceptual framework of electronic money laundering also encompasses a range of complex financial operations, including electronic transfers, the use of shell companies or multiple accounts, and the exploitation of legal loopholes across national borders, making prosecution a significant challenge for traditional legal systems.

This conceptual framework is important because it defines the characteristics of cybercrime, identifies its methods and techniques, and highlights the associated risks. It also helps in understanding the relationship between technological innovation and financial crime, enabling researchers and legal practitioners to develop effective prevention and control strategies. Among the most important characteristics highlighted by this framework are: the international reach of the crime, the speed with which financial transactions are executed, the difficulty in identifying criminals and their identities, and the use of advanced technologies to conceal the traces of transactions.

On the other hand, the conceptual framework of electronic money laundering is linked to a number of related concepts, such as organized financial crime, cybercrime, illicit finance, and illicit investment. A precise understanding of these concepts is the cornerstone for developing international and national legislative and legal frameworks capable of addressing the challenges of digital financial crime.

This section of the study addresses the legal basis for combating electronic money laundering (2.1), before referring to scholarly attempts to define the concept (2.2).

2.1. The legal basis for combating electronic money laundering:

Electronic money laundering represents one of the most complex forms of crime, both internationally and nationally, and is considered by some legal experts to be among the most dangerous. Despite this, this type of practice has not been defined within the framework of the most important relevant international conventions¹. In this regard, reference should be made initially to the United Nations Convention to Adopt a Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988, whose drafters addressed the issue indirectly in the context of Article 1, specifically within the framework of defining the terms used in the Convention, as is the case with regard to “proceeds,” which means “any funds derived or obtained, directly or indirectly, from the commission of an offence provided for in paragraph 1 of Article 3”². They also explicitly criminalized: The transferring or moving funds knowing that they are derived from any crime or crimes stipulated in subparagraph (a) of this paragraph, or from an act of participation in such crime or crimes, with the purpose of concealing or disguising the illicit source of the funds or with the intent to help any person involved in the commission of such crime or crimes to evade the legal consequences of his acts; in addition of concealing or disguising the true nature, source, status, disposition, movement, rights, or ownership of funds, knowing that they are derived from a crime or crimes stipulated in subparagraph (a) of this paragraph, or from an act of participation in such crime or crimes³ like The production, manufacture, extraction; preparation, offering, offering for sale, distribution, sale, delivery on any terms whatsoever, brokerage, dispatch, dispatch in transit, transport, importation or exportation of any narcotic drug or any psychotropic substance⁴.

This stance has been criticized for the narrow perspective adopted by the drafters of the convention; it punishes anyone who commits money laundering, provided they knew the criminal source of the funds at the

time of the act. However, they restrict money laundering to the proceeds of drug trafficking and related activities, excluding proceeds from other crimes⁵.

The Declaration of Principles on the Prevention of Money Laundering, issued by the Basel Committee in 1988, is one of the most important international texts in the field of combating money laundering. It defines the crime as: “all banking transactions intended to conceal the criminal origin of funds.” This definition has not been without its critics because it limits money laundering to banking transactions, whereas bank transfers, for example, are a means used to commit crimes. Furthermore, it limits the purpose of money laundering to concealment, whereas the true purpose of laundering is to legitimize the proceeds of a criminal act, such as bank robbery or drug trafficking—in other words, to legalize criminal proceeds⁶.

The European Commission on Money Laundering started from the criticisms mentioned above in order to develop a compromise definition of the crime of money laundering, and this is what it actually did within the framework of the guide it issued in its 1990 guide, which stated the following: The transfer of funds obtained from criminal activities, with the aim of concealing or disguising the illegal and prohibited source of these funds, or assisting any person who has committed a crime to avoid legal responsibility for the proceeds of this crime...⁷. Its conciliatory nature stems from the generality that characterized its wording, encompassing criminal proceeds from all illicit practices, whatever their nature. On the other hand, it did not limit the method of money laundering to a single form, but rather referred to all means that could evade legal responsibility for possessing the proceeds of illicit conduct⁸.

2.2. Electronic money laundering as a new form of cybercrime:

The ambiguity that may surround a legal rule is a double-edged sword; on the one hand, the gaps surrounding it can be

exploited by perpetrators to commit illegal acts, and on the other hand, the lack of precision would give the judge sufficient discretion to deal with all emerging circumstances; which allows us to acknowledge that electronic money laundering is included within the framework of the definition adopted by the countries participating in the adoption of the United Nations Convention against Transnational Organized Crime, which is taken as a basic model in the field of defining the concept of money laundering, and whose Article 6 states the following: « 1. Each State Party shall adopt, in accordance with fundamental principles of its domestic law, such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally:

(a) (i) The conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her action;

(ii) The concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime;... »⁹. An analysis of paragraph 1-2 of the above article reveals that its drafters did not specify a particular method of concealment or disguise, making electronic money laundering a likely and probable possibility. This latter, being relatively new, has not yet received a legal definition within the existing legal framework for combating this type of crime. This has prompted significant efforts at the doctrinal level to fill the existing gap in this area. In this regard, it is worth noting the definition provided by the Middle East and North Africa Financial Action Task Force (MENAFATF), which defined money laundering via electronic means as: A process or set of processes through which sophisticated monetary and financial systems are used to legitimize

funds obtained from an illicit source via the internet or other similar means in this context¹⁰.

In their definition of the crime of electronic money laundering, (Nur Afiah MD Amin and others) focus on its broad scope and multiple dimensions. They see it as committing money laundering through the use of electronic means via the Internet or through engaging in electronic exchanges, as these exchanges provide diverse options, fast transactions, and low fees. It is a multidisciplinary approach that includes expertise in the field of criminology, cybersecurity, economics, and law, where perpetrators exploit the complex nature of electronic justice in order to carry out and commit their money laundering-related crimes in the best possible way¹¹.

Like cryptocurrencies and electronic money, they are used to launder almost all types of criminal proceeds. These activities range from laundering digital proceeds, such as those used to pay ransoms or fund criminal infrastructure, to converting large sums of cash into virtual assets. Examples of cryptocurrency use in money laundering schemes include criminal networks purchasing cryptocurrencies with illicit proceeds and using them to transfer funds¹².

3. International cooperation in combating cyber money laundering crimes:

International cooperation constitutes a fundamental pillar in combating cyber money laundering crimes, given their transnational nature and the complexity of digital financial transactions. The rapid development of information and communication technologies has enabled criminal networks to exploit cyberspace to conceal illicit proceeds and transfer them across jurisdictions. Consequently, individual state efforts are often insufficient to effectively address these sophisticated crimes. International cooperation facilitates the exchange of information, mutual legal assistance, extradition of offenders, and coordination among law enforcement and financial intelligence units. It is further strengthened through international

conventions, regional frameworks, and the standards established by organizations dedicated to anti-money laundering efforts. Therefore, enhancing international collaboration remains essential to ensuring an effective and comprehensive response to cyber money laundering activities.

This section of the study addresses the measures of international cooperation included, whether within the framework of international agreements (3.1), or in the recommendations of the Financial Action Task Force (3.2).

3.1. In the framework of international treaties related to fight money laundering:

With the rapid development of digital technology, electronic money laundering has become one of the most dangerous transnational crimes, given its unprecedented ability to transcend geographical and legal boundaries. The use of tools such as digital wallets, cryptocurrency trading platforms, online banking, and anonymous communication networks has enabled criminal groups to transfer illicit funds between multiple countries in record time, with the perpetrators remaining largely untraceable. This transforms the crime from a limited, local activity into an interconnected network that exploits the disparity in legislation between countries and the weakness of international coordination. Consequently, electronic money laundering has become a global security challenge that threatens the integrity of financial systems and undermines national efforts to combat organized crime and the financing of terrorism, making its confrontation a shared responsibility that transcends the capacity of any single nation¹³.

The international community recognized this advantage at a later stage in the development of international regulations, dedicating entire sections to the issue in international treaties and conventions related to combating money laundering. This is exemplified by the Council of Europe Convention on Money Laundering, Control,

Tracing and Confiscation of the Proceeds of Crime of 1990, which includes a full chapter on international cooperation. Among its key provisions is the need to establish general principles and consistent measures for cooperation among members of the international community who coordinate their efforts to combat money laundering in the areas of investigation and procedures aimed at confiscating criminal proceeds and the means used to commit the crime¹⁴. In this regard, harmonizing various national legislations is a fundamental step towards successfully realizing this ethical objective in practice¹⁵.

The drafters of the United Nations Convention against Cybercrime address more precisely the measures that correspond to the crime of electronic money laundering, and they obligate States Parties to the international convention to cooperate effectively in the following areas: «1. States Parties shall cooperate with each other in accordance with the provisions of this Convention, as well as other applicable international instruments on international cooperation in criminal matters, and domestic laws, for the purpose of: (a) The investigation and prosecution of, and judicial proceedings in relation to, the criminal offences established in accordance with this Convention, including the freezing, seizure, confiscation and return of the proceeds from such offences; (b) The collecting, obtaining, preserving and sharing of evidence in electronic form of criminal offences established in accordance with this Convention; (c) The collecting, obtaining, preserving and sharing of evidence in electronic form of any serious crime, including serious crimes established in accordance with other applicable United Nations conventions and protocols in force at the time of the adoption of this Convention»¹⁶.

International cooperation also includes the commitment of States Parties to the International Convention on Mutual Legal Assistance, whereby they provide each other with the widest possible legal

assistance in investigations, prosecutions, and judicial proceedings related to offenses criminalized under this Convention, as well as in the collection of evidence in electronic form¹⁷. Mutual legal assistance naturally takes place within a legal framework defined by the laws of the States concerned and by relevant agreements and treaties pertaining to investigations, prosecutions, and judicial proceedings related to offenses for which a legal entity may be held accountable¹⁸.

In practice, mutual legal assistance includes a range of aims and purposes, the most important of which are: (a) obtaining evidence or statements from persons; (b) serving judicial documents; (c) carrying out searches, seizures and freezing; (d) inspecting, similarly accessing and disclosing data stored by an information technology system; (g) examining objects and sites; (h) providing information, evidence and expert assessments; (i) providing the originals of relevant documents and records, including governmental, banking, financial, corporate or business records, or certified copies thereof; (j) investigating or tracing the proceeds of crime, property, instruments or other objects for the purpose of obtaining evidence; (k) facilitating the voluntary appearance of persons in the requesting State Party; (l) recovering the proceeds of crime¹⁹.

The recovery of assets is one of the most significant challenges facing the international community in combating cyber money laundering. In this regard, States Parties are obligated to:

(a) Take the necessary measures to enable their competent authorities to enforce a confiscation order issued by a court in another State Party;

(b) Take the necessary measures to enable their competent authorities, where they have jurisdiction, to order the confiscation of assets of foreign origin through a judicial ruling in a money laundering or other similar offense within their jurisdiction, or through other

procedures authorized by their domestic law;

(c) Consider taking the necessary measures to enable the confiscation of such assets without a criminal conviction in cases where the perpetrator cannot be prosecuted due to death, flight, absence, or other appropriate circumstances²⁰.

3.2. In the recommendations of the Financial Action Task Force:

The recommendations of the Financial Action Task Force constitute the cornerstone of the international framework for combating money laundering, terrorist financing, and the financing of proliferation. They provide a comprehensive set of legal, institutional, and operational standards designed to strengthen national anti-financial crime regimes. These recommendations encourage states to adopt risk-based approaches, enhance transparency of beneficial ownership, and ensure effective supervision of financial institutions. They also emphasize international cooperation, mutual legal assistance, and information exchange among competent authorities. Through periodic evaluations, the recommendations promote compliance and continuous improvement of national systems. Consequently, the FATF Recommendations have become globally recognized benchmarks for safeguarding the integrity and stability of the international financial system.

This section of the study addresses international cooperation (3.2.1), confiscation (3.2.2), and finally, matters related to combating terrorism and financing proliferation (3.2.3).

3.2.1. General aspects of international cooperation:

International cooperation measures developed by the Financial Action Task Force (FATF) constitute a fundamental pillar of the global framework for combating money laundering, terrorist financing, and the proliferation of weapons of mass destruction. Recognizing the transnational nature of financial crimes, the FATF has established comprehensive standards that

encourage states to strengthen mutual legal assistance, extradition mechanisms, information exchange, and cooperation among financial intelligence units, supervisory authorities, law enforcement agencies, and judicial bodies. In particular, Recommendations 36 to 40 emphasize the necessity of implementing effective international cooperation mechanisms by ensuring the timely sharing of financial and investigative information, facilitating asset tracing, freezing, seizure, and confiscation procedures, and promoting collaborative investigations across jurisdictions. The FATF also supports international cooperation through its peer-review process, known as mutual evaluations, which assesses countries' compliance with international standards and identifies deficiencies requiring corrective measures. Furthermore, the organization cooperates closely with regional bodies and international institutions to enhance technical assistance, capacity building, and the harmonization of national legal frameworks. These measures contribute significantly to reducing regulatory gaps, improving the detection and prosecution of transnational financial crimes, and fostering a coordinated global response to increasingly sophisticated illicit financial activities²¹.

3.2.2. Confiscation:

Money laundering and confiscation are intrinsically linked components of contemporary criminal justice policies aimed at combating organized crime and illicit financial activities. Money laundering refers to the process by which individuals or criminal organizations conceal the illicit origin of proceeds derived from predicate offenses, integrating them into the legitimate financial system to obscure their unlawful source and facilitate their use without attracting suspicion. Confiscation, on the other hand, constitutes a legal measure that enables competent authorities to permanently deprive offenders of assets, proceeds, instrumentalities, or property connected to criminal activities. The

effectiveness of confiscation as a deterrent mechanism lies in its ability to undermine the economic foundations of criminal enterprises by removing the financial incentives that motivate illicit conduct. International legal instruments, particularly United Nations conventions and the recommendations of the Financial Action Task Force, emphasize the necessity of adopting comprehensive confiscation regimes, including value-based confiscation, extended confiscation, and non-conviction-based confiscation where compatible with domestic legal systems. Consequently, robust confiscation frameworks are widely regarded as indispensable tools for disrupting money laundering schemes, recovering criminal assets, and reinforcing the integrity and stability of national and international financial systems²².

3.2.3. Terrorist financing and financing of proliferation:

Terrorist financing and the financing of proliferation represent serious threats to international peace, security, and the integrity of the global financial system. Terrorist financing refers to the collection, movement, or provision of funds, assets, or financial services intended to support terrorist acts, individual terrorists, or terrorist organizations, regardless of whether such resources originate from lawful or unlawful sources. In contrast, the financing of proliferation involves providing funds or financial services that facilitate the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling, or use of nuclear, chemical, or biological weapons and their means of delivery, particularly in violation of international obligations and sanctions regimes. The transnational and clandestine nature of these activities necessitates robust preventive and repressive measures, including targeted financial sanctions, enhanced customer due diligence, monitoring of suspicious transactions, and effective mechanisms for international cooperation and information exchange. International standards developed

by the Financial Action Task Force, together with binding obligations established under the United Nations framework, require States to criminalize terrorist financing, implement measures to prevent the financing of proliferation, and strengthen institutional capacities to detect, investigate, and prosecute such offenses. By depriving terrorists and proliferators of access to financial resources, these measures contribute significantly to maintaining international security and preventing the spread of weapons of mass destruction²³.

4. Conclusion:

In conclusion, this study on combating electronic money laundering in international law demonstrates that rapid technological advancements and the accompanying expansion in the use of digital media and electronic financial services have created unprecedented legal and security challenges, making electronic money laundering one of the most serious contemporary economic and financial crimes. The digital environment has provided criminals with more sophisticated and flexible means to conceal the illicit sources of funds and transfer them across borders with unprecedented speed, exploiting technological development, the proliferation of digital platforms, and the difficulty of subjecting cyberspace to unified and effective legal oversight.

The study revealed that electronic money laundering is not merely a technological evolution of traditional money laundering, but rather a new criminal pattern characterized by distinct features, most notably its speed, flexibility, transnational nature, and reliance on modern technologies such as cryptocurrencies, digital transfers, and encryption techniques. This makes combating it a challenge that transcends national jurisdiction and requires a comprehensive international legal response. The study also revealed that international efforts in this area, despite their importance, still face numerous difficulties related to the disparity of national legislation, weak international coordination, and the rapid

evolution of criminal methods beyond the capacity of traditional laws to keep pace.

An analysis of international legal frameworks reveals that the international community has sought to establish a legal system aimed at mitigating the risks of this crime through the adoption of international treaties and conventions and multilateral cooperation mechanisms. Among the most prominent of these is the United Nations Convention against Transnational Organized Crime. Furthermore, the Financial Action Task Force plays a pivotal role by developing international recommendations and standards that promote financial transparency and criminalize money laundering and terrorist financing. International cooperation, whether through information exchange, judicial assistance, or security coordination, has proven to be a cornerstone for ensuring the effectiveness of efforts to detect cyber financial crimes, track down perpetrators, and recover criminal proceeds.

However, the effectiveness of combating cyber money laundering remains contingent upon countries' ability to develop their national legislation and update their regulatory mechanisms to keep pace with rapid digital transformations. This also necessitates strengthening international coordination, exchanging technical expertise, and adopting artificial intelligence systems and modern technologies to monitor suspicious transactions. A comprehensive approach is also required, one that integrates legal, technical, and institutional aspects to achieve a balance between the requirements of financial security and respect for digital rights and freedoms.

Therefore, confronting electronic money laundering is no longer just a legislative or political option, but has become an international necessity imposed by the nature of the global digital economy, which calls for concerted international, regional and national efforts to build a more flexible and effective legal system capable of addressing emerging risks and ensuring the protection of economic and financial

stability at the national and international levels.

Study results:

The study on combating electronic money laundering in international law reached a number of key findings, which can be summarized as follows:

-The study demonstrated that electronic money laundering is a newly emerging financial crime whose emergence is linked to technological development and the widespread adoption of digital transactions. Electronic means have become a fertile ground for concealing and disguising the sources of illicit funds in a more sophisticated manner compared to traditional methods;

-The study showed that the crime of electronic money laundering is characterized by several features, most notably the speed of executing financial transactions, its transnational nature, and the difficulty of tracing and proving it. Furthermore, it exploits modern technologies such as cryptocurrencies and electronic payment platforms, which complicates the task of regulatory and judicial bodies;

-The study revealed that the international legal framework for combating electronic money laundering is based on a set of international treaties and conventions and standards aimed at strengthening international cooperation and criminalizing money laundering. Among the most prominent of these are the United Nations Convention against Transnational Organized Crime, along with the standards and recommendations issued by the Financial Action Task Force (FATF). The study demonstrated that international cooperation is the cornerstone of combating cyber money laundering, given the transnational nature of this crime. Information exchange, mutual legal assistance, and security coordination among countries are among the most important mechanisms for enhancing the effectiveness of these efforts;

-The study also identified legal and technical challenges that limit the effectiveness of international efforts. These include differing

national legislation, weak international coordination, the proliferation of secure digital havens, and the difficulty of monitoring financial transactions involving cryptocurrencies and modern encryption technologies;

-The study emphasized that traditional legislation is no longer sufficient to address rapid technological advancements. This necessitates updating national laws and adapting them to digital developments, as well as strengthening oversight of electronic financial institutions;

-The study concluded that the effectiveness of combating cyber money laundering remains contingent on the international community's ability to develop more flexible and effective cooperation mechanisms. These mechanisms should be based on unifying legal, technical, and institutional efforts to address emerging risks that threaten the security and stability of the global financial system.

Recommendations:

Based on the findings of this study on combating electronic money laundering in international law, a set of academic recommendations, supported by practical legal alternatives, can be proposed as follows:

-The need to review and update national anti-money laundering laws to align with modern technological developments, particularly those related to digital financial transactions, cryptocurrencies, and electronic payment platforms. This can be achieved by introducing independent legal texts that explicitly criminalize various forms of electronic money laundering, along with a precise legal definition of this crime, its elements, and the mechanisms for digital proof;

-The need to intensify international cooperation in the exchange of information and technical and judicial expertise to address the transnational nature of electronic money laundering crimes. This can be accomplished through the conclusion of specialized international and regional agreements or the development of existing

agreements to establish mandatory mechanisms for judicial cooperation and more effective exchange of electronic financial data;

-The need to impose stricter legal and institutional oversight on digital assets, trading platforms, and electronic wallets that may be exploited in money laundering operations. This can be achieved by subjecting virtual asset service providers to a rigorous licensing and legal oversight system, and obligating them to implement customer identity verification and suspicious transaction reporting rules in accordance with international standards issued by the Financial Action Task Force;

-The need to update the means of investigation and inquiry into electronic financial crimes, and to provide the competent authorities with the modern technologies necessary to track suspicious digital funds, and to create specialized judicial and security units for electronic financial crimes, while adopting the validity of digital evidence and developing the rules of electronic proof within procedural legislation;

- Intensify training programs for judges, law enforcement agencies, and financial institutions to enhance their understanding of electronic money laundering mechanisms and evolving methods. This can be achieved by imposing a legal obligation on financial institutions and regulatory bodies to conduct regular training courses for their staff in financial compliance and cybersecurity;

-Establish an international mechanism for exchanging information on suspicious electronic financial activities. This will contribute to the rapid detection of transnational crimes. Such a mechanism could be established through an international legal platform, under the auspices of the United Nations or in coordination with Interpol, dedicated to exchanging information related to electronic money laundering crimes, while respecting data protection and privacy regulations;

-Ensure that digital rights and freedoms are not infringed upon when implementing

measures to combat electronic money laundering. This requires enacting clear legal safeguards that define the controls for collecting and monitoring digital financial data, guaranteeing respect for the right to privacy and preventing the arbitrary use of electronic surveillance tools.

5. BIBLIOGRAPHY LIST:

A-ARTICLES:

1-Chad Albrecht, Kristopher McKay Duffin, Conan Albrecht, Victor manuel morales Rocha, «The use of cryptocurrencies in the money laundering process», journal of money laundering control, vol.22, N°02, 2019.

2-Jean-Francois Thony, Money laundering and terrorism financing: An overview, in: Current development in monetary and financial law, Vol.3, International monetary fund, 29 April 2005.

3-Muhammad Saleem Korejo, The concept of money laundering: a quest for legal definition, Journal of money laundering control, Vol.24, N°04, 2021.

4-Norman Mugarura and Emma Ssali, Intricacies of anti-money laundering and cyber-crimes regulatio in a fluid global system, Vol.88, Issue 6, 10 November 2025.

5-Nur Afiqah MD Amin and others, Cyber-laundering and its impacts on auditors: A conceptual paper, accounting and finance research, Vol.13, N°02, 2024.

6-Valsamis Mitsilegas and Bill Gilmore, The EU legislative framework against money laundering and terrorist finance: A critical analysis in the light of evolving global standards, International and comparative law quarterly, Vol.56, January 2007.

B-LEGAL TEXTS:

-INTERNATIONAL TEXTS:

1-Council of Europe, convention on laundering, search, seizure and confiscation of the proceeds from crime, European treaty series, N°141, Strasbourg, November 8th, 1990.

2-«On prevention of the use of the financial system for the purpose of money laundering», ref: 91/308/EEC, official

journal of the european communities, N° L 166/77, of 28 June 1991.

3-United Nations Convention against Transnational Organized Crime, adopted and opened for signature, ratification and accession by United Nations General Assembly resolution 25 (fifth session) of 15 November 2000.

4-United Nations convention against cybercrime; strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for sharing of evidence in electronic form of serious crimes. Adopted in the framework of the General assembly resolution A/RES/79/243 of 31st December 2024.

5-Financial Action Task Force, International standards on combating money laundering and the financing of terrorism & proliferation, the FATF recommendations, Paris, France, October 2025.

NATIONAL TEXT:

-Décret présidentiel N°95-41 du 26 Chaabane 1415 correspondant au 28 janvier 1995 portant ratification, avec réserve de la convention des Nations Unies contre le trafic illicite des stupéfiants et des substances psychotropes, adoptée à vienne le 20 Décembre 1998, Journal officiel de la république Algérienne, N°7 du 15 février 1995.

C-REPORTS:

1-Middle east and north africa financial action task force, Typologies report on: «money laundering and corruption», Manama, Kingdom of Bahrain, December 2017.

2-Europol, cryptocurrencies: tracing the evolution of criminal finances, Europol series, report series, Publications of office of the European union, Luxembourg, 2021.

6.Citations:

⁵-Muhammad Saleem Korejo, The concept of money laundering: a quest for legal definition, Journal of money laundering control, Vol.24, N°04, 2021, pp, 732-733.

⁶-Jean-Francois Thony, Money laundering and terrorism financing: An overview, in: Current development in monetary and financial law, Vol.3, International monetary fund, 29 April 2005, p 255.

⁷- Article 1, Para.3 from «On prevention of the use of the financial system for the purpose of money laundering», ref: 91/308/EEC, official journal of the european communities, N° L 166/77, of 28 June 1991.

⁸-Valsamis Mitsilegas and Bill Gilmore, The EU legislative framework against money laundering and terrorist finance: A critical analysis in the light of evolving global standards, International and comparative law quarterly, Vol.56, January 2007, p 129.

⁹-See: Article 6, Para. 1 from United Nations Convention against Transnational Organized Crime, adopted and opened for signature, ratification and accession by United Nations General Assembly resolution 25 (fifth session) of 15 November 2000.

¹⁰-See: Middle east and north africa financial action task force, Typologies report on: «money

¹-Norman Mugarura and Emma Ssali, Intricacies of anti-money laundering and cyber-crimes regulatio in a fluid global system, Vol.88, Issue 6, 10 November 2025, p 5.

²-See: Article 1 du Décret présidentiel N°95-41 du 26 Chaabane 1415 correspondant au 28 janvier 1995 portant ratification, avec réserve de la convention des Nations Unies contre le trafic illicite des stupéfiants et des substances psychotropes, adoptée à vienne le 20 Décembre 1998, Journal officiel de la république Algérienne, N°7 du 15 février 1995.

³-Article 3, Para.1 (b) '1' et '2' du Décret présidentiel N°95-41 du 26 Chaabane 1415 correspondant au 28 janvier 1995 portant ratification, avec réserve de la convention des Nations Unies contre le trafic illicite des stupéfiants et des substances psychotropes, adoptée à vienne le 20 Décembre 1998, Op. Cit.

⁴-Article 3, Para.1 (a) du Décret présidentiel N°95-41 du 26 Chaabane 1415 correspondant au 28 janvier 1995 portant ratification, avec réserve de la convention des Nations Unies contre le trafic illicite des stupéfiants et des substances psychotropes, adoptée à vienne le 20 Décembre 1998, Op. Cit.

¹⁹-Article 40, Para. 3 from the United Nations convention against cybercrime; strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for sharing of evidence in electronic form of serious crimes. Adopted in the framework of the General assembly resolution A/RES/79/243 of 31st December 2024.

²⁰-Article 49, Para. 1 from the United Nations convention against cybercrime; strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for sharing of evidence in electronic form of serious crimes. Adopted in the framework of the General assembly resolution A/RES/79/243 of 31st December 2024.

²¹-See: Recommendation 30-40 from Financial Action Task Force, International standards on combating money laundering and the financing of terrorism & proliferation, the FATF recommendations, Paris, France, October 2025, pp, 27-30.

²²-See: Recommendation 1-3 from Financial Action Task Force, International standards on combating money laundering and the financing of terrorism & proliferation, the FATF recommendations, Paris, France, October 2025, p 12.

²³-See: Recommendation II and III and VIII from Financial Action Task Force, International standards on combating money laundering and the financing of terrorism & proliferation, the FATF recommendations, Paris, France, October 2025, p 13.

laundrying and corruption», Manama, Kingdom of Bahrain, December 2017, p 29.

¹¹-Nur Afifah MD Amin and others, Cyber-laundering and its impacts on auditors: A conceptual paper, accounting and finance research, Vol.13, N°02, 2024, p 24.

¹²-Europol, cryptocurrencies: tracing the evolution of criminal finances, Europol series, report series, Publications of office of the European union, Luxembourg, 2021, p 21.

¹³-Chad Albrecht, Kristopher McKay Duffin, Conan Albrecht, Victor manuel morales Rocha, «The use of cryptocurrencies in the money laundering process», journal of money laundering control, vol.22, N°02, 2019, pp, 214-216.

¹⁴-Article 7 para.1 from Council of Europe, convention on laundrying, search, seizure and confiscation of the proceeds from crime, European treaty series, N°141, Strasbourg, November 8th, 1990.

¹⁵-Article 7 para.2 from Council of Europe, convention on laundrying, search, seizure and confiscation of the proceeds from crime, European treaty series, N°141, Strasbourg, November 8th, 1990.

¹⁶-Article 35, Para.1- from the United Nations convention against cybercrime; strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for sharing of evidence in electronic form of serious crimes. Adopted in the framework of the General assembly resolution A/RES/79/243 of 31st December 2024.

¹⁷- Article 40, Para. 1 from the United Nations convention against cybercrime; strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for sharing of evidence in electronic form of serious crimes. Adopted in the framework of the General assembly resolution A/RES/79/243 of 31st December 2024.

¹⁸-Article 40, Para. 2 from the United Nations convention against cybercrime; strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for sharing of evidence in electronic form of serious crimes. Adopted in the framework of the General assembly resolution A/RES/79/243 of 31st December 2024.