



وزارة التعليم العالي والبحث العلمي

جامعة عبد الحفيظ بوالصوف - ميله

كلية الحقوق

الرقم التسلسلي:

القسم: الحقوق

الرمز:

التخصص: قانون أعمال

الجريمة الاقتصادية في البيئة الرقمية

(جريمة تبويض الأموال نموذجاً)

مذكرة ضمن متطلبات نيل شهادة

(الماستر)

إشراف الأستاذة:

إعداد الطلبة:

مريم بوزرارة زقار

بن ناصر بدر الدين

حمدوني رضا

السنة الجامعية: 2026/2025



وزارة التعليم العالي والبحث العلمي

جامعة عبد الحفيظ بوالصوف - ميله

كلية الحقوق

الرقم التسلسلي:

القسم: الحقوق

الرمز:

التخصص: قانون أعمال

الجريمة الاقتصادية في البيئة الرقمية

(جريمة تبييض الأموال نموذجاً)

مذكرة ضمن متطلبات نيل شهادة

(الماستر)

إشراف الأستاذة:

إعداد الطلبة:

مريم بوزرارة زقار

بن ناصر بدر الدين

حمدوني رضا

أعضاء لجنة المناقشة:

. موسى زينب جامعة عبد الحفيظ بوالصوف ميله (أستاذ محاضر أ) رئيساً .

. مريم بوزرارة زقار جامعة عبد الحفيظ بوالصوف ميله (أستاذ مساعد) مشرفاً ومقرراً .

. عيلوط زكريا جامعة عبد الحفيظ بوالصوف ميله (أستاذ مساعد) عضواً مناقشاً .

السنة الجامعية: 2025/2026

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

ملخص الدراسة باللغة العربية:

شهد العالم المعاصر تحولاً جذرياً نحو الرقمنة الشاملة، وهو ما انعكس إيجاباً على كفاءة المعاملات المالية، ولكنه أدى في المقابل إلى ظهور أنماط مستحدثة من الجريمة المنظمة، وفي مقدمتها جريمة تبييض الأموال في البيئة الرقمية، حيث تُعرف هذه الجريمة بأنها سلوك إجرامي تقني يعتمد على استغلال التطور التكنولوجي والتدفقات المالية الافتراضية لإخفاء المصدر غير المشروع للأموال المستمدة من أنشطة محظورة قانوناً، وإعادة دمجها في الاقتصاد الرسمي لتبدو كأنها أرباح شرعية، وتتميز هذه الظاهرة الإجرامية باعتمادها على آليات تكنولوجية معقدة تتجاوز الأساليب التقليدية؛ حيث تمر بثلاث مراحل متداخلة ومطورة رقمياً تبدأ بالإيداع عبر منصات التداول والمحافظ الإلكترونية، ثم التمويل والتغطية من خلال شبكة معقدة من التحويلات الخاطفة واستخدام أدوات إخفاء الهوية، وصولاً إلى مرحلة الدمج النهائي في النظام المالي التقليدي أو الرقمي، وتتعدد الوسائل المستخدمة في هذا النطاق، بدءاً من العملات المشفرة ذات الخصوصية العالية مروراً بالرموز غير القابلة للاستبدال (Nfts) وصولاً إلى منصات الألعاب الإلكترونية وبنوك الظل الرقمية وهي أدوات تمنح الجناة ميزة السرية المطلقة والسرعة الفائقة في التنفيذ، بناءً على ذلك تواجه لمنظومة القانونية والأمنية الدولية تحديات جسيمة لمكافحة هذه الجريمة، تتبلور في الطابع العابر للحدود الوطنية للبيئة الرقمية، وغياب الهوية الحقيقية للمتعاملين، فضلاً عن وجود فجوات تشريعية بين الدول، الأمر الذي يستلزم تحديث الاستراتيجيات الوقائية والعقابية من خلال تفعيل تقنيات الذكاء الاصطناعي في رصد المعاملات المشبوهة، وتشديد تدابير الامتثال والتحقق من الهوية الرقمية (KYC)، مع التأكيد على حتمية تعزيز التعاون الدولي القضائي والأمني لمواجهة هذا التهديد المتنامي للاقتصاد العالمي.

الكلمات المفتاحية: تبييض الأموال الرقمي، البيئة الرقمية، العملات المشفرة، جريمة، المنظومة القانونية.

الملخص باللغة الإنجليزية:

Abstract

The contemporary world has witnessed a radical shift toward comprehensive digitization, which has enhanced financial transaction efficiency but conversely led to the emergence of novel patterns of organized crime, cyber-enabled money laundering being chief among them. This crime is defined as a sophisticated technological misconduct that exploits advancements in financial technology and virtual financial flows to conceal the illicit origin of funds derived from illegal activities, ultimately reintegrating them into the formal economy as legitimate wealth. This criminal phenomenon is characterized by its reliance on intricate technical mechanisms that transcend traditional methods, operating through three interrelated and digitally enhanced stages: placement via trading platforms and electronic wallets; layering through a complex web of rapid transactions and anonymity-enhancing tools; and finally, integration into the mainstream or digital financial systems. The methods employed in this domain vary widely, ranging from privacy-centric cryptocurrencies and Non-Fungible Tokens (NFTs) to online gaming platforms and digital shadow banks tools that grant perpetrators total anonymity and hyper-speed execution. Consequently, global legal and security frameworks face formidable challenges in combating this crime, primarily due to the inherently borderless nature of the digital environment, the lack of real identity verification, and regulatory disparities across jurisdictions. Therefore, mitigating this growing threat to the global economy necessitates updating preventive and punitive strategies by deploying artificial intelligence to detect suspicious transactions, tightening Know Your Customer (KYC) digital compliance measures, and reinforcing international judicial and security cooperation.

Keywords: Digital Money Laundering, Digital Environment Cryptocurrencies Crime, Legal System.

شكر وتقدير

قال الله تعالى: " وإذ تأذن ربكم لئن شكرتم لأزيدنكم ولئن كفرتم إن عذابي لشديد " صدق الله العظيم

سورة إبراهيم -7-

في البداية نحمد الله عزوجل ونشكره على أن أنعم علينا بتوقيقه لإتمام هذا العمل، ومن علينا كذلك لإتمام

الخطوات الأخيرة في الحياة الجامعية بعد أعوام قضيناها في رحاب الجامعة مع أساتذتنا الأفاضل

ويقول النبي صلى الله عليه وسلم: " من لا يشكر الناس لا يشكر الله " نتقدم بجزيل الشكر والتقدير للأستاذة

"د/مريم بوزرارة زقار" التي تفضلت مشكورة بقبول الإشراف على هذا العمل والحرص على اكتماله وعن

المعلومات والإفادات والنصائح التي وجهتها لنا ومنحتها وقتها الثمين وكرمها الفياض، سواء من الناحية المنهجية

أو من ناحية المضمون العلمي، فلولاها لما رأى هذا العمل النور، راجيا المولى عزوجل أن يجعلها في ميزان حسناتها

كما نتقدم بالشكر والاحترام وعظيم التقدير للسادة الأفاضل أعضاء لجنة المناقشة، كل باسمه

الأستاذة القديرة موسى زينب، والأستاذ القدير: عيلوط زكريا

على تفضلهم بمناقشة المذكرة، وعلى ما بذلوه من جهد، وعلى ما أبدوه من ملاحظات قيمة بما يثري هذا العمل

الإهداء

بسم الله الرحمن الرحيم

"وانخفض لهما جناح الذل من الرحمة وقل رب ارحمهما كما ربياني صغيراً"

إلى والدي الكريمين حفظهما الله وأطال عمرهما

إلى أسرتي الفاضلة التي اعاننتني كثيرا

وإلى أقاربي الذين يفرحون لفرحي من قريب ومن بعيد

وإلى كل الأصدقاء المخلصين الذين كانوا عوناً لي

وإلى زملاء الدراسة الذين شاركت معهم أجواء الحياة الجامعية

إلى كل من أنار لي طريق العلم والمعرفة

إلى طلاب العلم

أهدي ثمرة هذا البحث لكم جميعاً، راجياً المولى عزوجل أن يحفظكم بحفظه ويمدكم بعونه وان يجمعني

وإياكم في جنات النعيم

الطالب: بن ناصر بدر الدين

إهداء

إلى من أبصرت بها طريق حياتي واعتزاني بذاتي .. إلى القلب الحنون .. إلى من كانت
دعواتها تحيطني

أمي الحبيبة

إلى النور الذي أضاء دربي، إلى العزيز الذي حملت اسمه فخرا، إلى معلمي الأول الرجل
الذي سعى طوال حياته لتكون الأفضل

أبي الغالي

إلى الذين كانوا دائما مصدر قوة وسند لي

إخوتي

إلى الذين كان لهم الفضل في تكوين العلم

أساتذتي

إلى الذين رافقوني خلال سنوات الدراسة

أصدقائي وزملائي

إلى كل من ساهم من قريب أو بعيد في إنجاز هذه المذكرة

قائمة المختصرات

الطبعة	ط
الصفحة	ص
من الصفحة إلى الصفحة	ص ص
الجزء	ج
دون بلد النشر	د ب ن
دون تاريخ النشر	د ت ن
دون طبعة	د ط
دون عدد	دع
دون دار نشر	د د ن
الجريدة الرسمية	ج ر

	فهرس المحتويات
2	مقدمة
5	الفصل الأول: الإطار المفاهيمي والتقني لجريمة تبييض الأموال في البيئة الرقمية
6	المبحث الأول: الإطار المفاهيمي لجريمة تبييض الأموال في ظل التحول الرقمي
7	المطلب الأول: ماهية جريمة تبييض الأموال في البيئة الرقمية
7	الفرع الأول: تعريف الجريمة الاقتصادية
8	الفرع الثاني: مفهوم جريمة تبييض الأموال في البيئة الرقمية
20	الفرع الثالث: مفهوم البيئة الرقمية.
22	المطلب الثاني: مراحل جريمة تبييض الأموال في ظل التحول الرقمي وخصائصها
22	الفرع الأول: مراحل جريمة تبييض الأموال في البيئة الرقمية
24	الفرع الثاني: خصائص جريمة تبييض الأموال في البيئة الرقمية
26	المبحث الثاني: الوسائل التقنية المستحدثة في عملية تبييض الأموال
26	المطلب الأول: العملات المشفرة كآلية لتبييض الأموال
26	الفرع الأول: مفهوم العملات المشفرة وانواعها
29	الفرع الثاني: خصائص العملات المشفرة
31	الفرع الثالث: آليات استخدامها في التمويه
34	المطلب الثاني: استغلال المنصات والوسائل الرقمية في تبييض الأموال
35	الفرع الأول: استغلال التجارة الإلكترونية في عملية تبييض الأموال
37	الفرع الثاني: تبييض الأموال عن طريق الألعاب الرقمية
38	الفرع الثالث: استخدام بنوك الأنترنت في عملية تبييض الأموال
38	الفرع الرابع: استخدام التحويل الإلكتروني للأموال في عملية تبييض الأموال
39	الفرع الخامس: استخدام بطاقات الدفع الذكية في عمليات تبييض الأموال

42	خلاصة الفصل الأول
43	الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة
44	المبحث الأول: الجهود الوطنية والدولية لمكافحة جريمة تبييض الأموال في البيئة الرقمية
45	المطلب الأول: الجهود الوطنية والتدابير الوقائية لمكافحة جريمة تبييض الأموال في البيئة الرقمية
45	الفرع الأول: الجهود الوطنية لمكافحة جريمة تبييض الأموال في البيئة الرقمية
58	الفرع الثاني: التدابير الوقائية
62	المطلب الثاني: الجهود الدولية لمكافحة جريمة تبييض الأموال
62	الفرع الأول: الاتفاقيات والمنظمات الدولية
67	الفرع الثاني: المبادرات والآليات متعددة الأطراف
69	المبحث الثاني: تحديات الإثبات والملاحقة في جريمة تبييض الأموال في البيئة الرقمية
70	المطلب الأول: إشكالية الدليل الرقمي وحجته التقنية في إثبات جريمة تبييض الأموال في البيئة الرقمية
70	الفرع الأول: تعريف الدليل الرقمي وخصائصه
72	الفرع الثاني: إشكالية قبول الدليل الرقمي في إثبات الجريمة الرقمية وحجته التقنية
76	المطلب الثاني: عوائق الملاحقة القضائية لجريمة تبييض الأموال في البيئة الرقمية
76	الفرع الأول: المعوقات المتعلقة بخصوصية الدليل الرقمي
81	الفرع الثاني: المعوقات المتعلقة بخصوصية التحقيق
86	خلاصة الفصل الثاني:
88	خاتمة
92	قائمة المصادر والمراجع

مقدمة

إن من أهم التحديات وأخطرها التي واجهها ولا يزال يواجهها المجتمع الدولي الجريمة الاقتصادية كونها لا تستهدف الأفراد بشكل مباشر فحسب، بل تضرب في عمق الاستقرار المالي والمؤسساتي للدول حيث باتت معوقا أساسيا للبرامج التنموية محليا وقاريا، ومثلما ساهم التطور التكنولوجي في تطور وانتعاش الاقتصاد ساهم في ظهور أنماط وأنواع وصور جديدة من الجرائم الاقتصادية نتيجة للثورة التكنولوجية والرقمية والعولمة وعلى رأسها جريمة تبييض الأموال في البيئة الرقمية، وتتخذ هذه الجرائم أنماطا متطورة ومستمرة التغير مما يمنحها طابعا عابرا للحدود في كثير من الأحيان، ولا تقتصر أثارها المدمرة على الخسائر المادية الجاسمة، بل تمتد إلى لتقويض مناخ الاستثمار، وإضعاف الثقة في النظام المصرفي، وتعطيل مسارات التنمية المستدامة.

فجريمة تبييض الأموال أصبحت أكثر تعقيدا نتيجة استخدام التقنيات الحديثة لإخفاء مصدر الأموال المحصلة بطريقة غير قانونية، مما دفع المجتمع الدولي إلى تكثيف جهوده لوضع آليات قانونية ومؤسساتية لمواجهة، عبر إبرام اتفاقيات دولية وتشريع قوانين وطنية تهدف للحد منها ومكافحة صورها المتجددة في الفضاء الرقمي.

لهذا تم اختيارنا لهذا الموضوع، لأسباب ذاتية وأخرى موضوعية، فالأسباب الذاتية تتعلق برغبة الباحث في تسليط الضوء على جريمة مستحدثة وأهميتها المتزايدة في ظل التطور الرقمي، أما عن الأسباب الموضوعية فهي تتمثل أساساً في قلة الدراسات المتخصصة التي تناولت الموضوع من الناحية القانونية، مما دفع إلى محاولة الإحاطة بمختلف جوانبه وتحليل آليات مكافحته، إضافة إلى خطورة جريمة تبييض الأموال على الاقتصاد والمجتمع باعتبارها جريمة باتت تؤرق المجتمع الجزائري والدولي.

ونظرا لخطورة هذه جريمة في البيئة الرقمية، تتجلى الأهمية العلمية والعملية لهذه الدراسة كموضوع جدير بالبحث والتحليل في:

مدى فعالية الإطار القانوني المعتمد لمواجهة، خاصة في ظل التطور المستمر للوسائل الإلكترونية المستعملة في ارتكابها.

نظراً لاتساع نطاق الجرائم الاقتصادية المرتبطة بالبيئة الرقمية، تم اختيار جريمة تبييض الأموال الرقمية كنموذج للدراسة، باعتبارها من أكثر الجرائم تعقيداً من حيث آليات التنفيذ والإثبات والملاحقة، كذلك الاهتمام المتزايد الذي أولته مختلف الدول والمنظمات الدولية للجرائم المرتبطة بالبيئة الرقمية، وعلى رأسها

مقدمة

جريمة تبييض الأموال، بخلاف أنها من أخطر الجرائم الاقتصادية المعاصرة لما تخلفه من آثار سلبية على الاقتصاد الوطني والاستقرار المالي والأمني والاجتماعي.

كما تتجلى أهمية الدراسة في محاولة الإحاطة بجريمة تبييض الأموال في البيئة الرقمية من خلال التعرف على الوسائل والتقنيات الحديثة المستعملة في ارتكابها، فضلاً عن إبراز الصعوبات التي تواجه الجهات المختصة في كشفها وتعقب مرتكبيها، وتسلط الضوء على مدى فعالية الآليات القانونية والمؤسسية المعتمدة لمكافحة هذه الجريمة، سواء على المستوى الوطني أو الدولي، خاصة في ظل التطور التكنولوجي المتسارع الذي أفرز صوراً وأساليب جديدة لتبييض الأموال عبر البيئة الرقمية.

يتوخى هذا البحث تحقيق جملة من الأهداف على رأسها:

بيان مفهوم جريمة تبييض الأموال في البيئة الرقمية وخصائصها وتحديد الأفعال المكونة للجريمة وأركانها القانونية، بالإضافة إلى إبراز دور المؤسسات المالية المصرفية في مكافحة هذه الجريمة، وتوضيح الصعوبات التي تواجه آليات مكافحة تبييض الأموال الرقمية فضلاً عن دراسة الجهود التشريعية الوطنية والدولية الرامية إلى الحد منها فقد وضعت الجزائر نظاماً قانونياً ومؤسسياً؛ من خلال تبني الاتفاقيات الدولية وسن التشريعات الوطنية لاسيما القانون رقم 25-10 المؤرخ في 24 يوليو 2025، يعدل ويتم القانون رقم 05-01 المؤرخ في 6 فبراير 2005، المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتها، ومن جهة أخرى تم إنشاء خلية معالجة الاستعلام المالي التي تلعب دوراً محورياً ضمن المنظومة التي تضطلع بالوقاية من الجريمة ومكافحتها، بالإضافة إلى اتخاذ حزمة من الإجراءات في المجال المالي والمصرفي على وجه الخصوص فإن تكييف منظومة مكافحة تبييض الأموال في الجزائر وفقاً للمعايير الدولية، أضحى السبيل الأمثل لمكافحة فعالة على المستوى الوطني، ولبنة مهمة في سياق البنيان الدولي ككل في هذه المعركة.

ومن هنا يمكن طرح الإشكالية التالية: كيف ساهمت البيئة الرقمية في تطور الجريمة الاقتصادية وتغير آلياتها التقليدية، إلى أي مدى استجابت المنظومة القانونية والرقابية لمواجهة هذا التحول الإجرامي باتخاذ جريمة تبييض الأموال الرقمية كنموذج يجسد تحديات الملاحقة والوقاية؟

واعتباراً لطبيعة الموضوع فإن المناهج المتبعة للدراسة هي: المنهج الوصفي والمنهج التحليلي لأنه الأنسب لموضوعنا، ولأنه السبيل لتحقيق هذه الدراسة لأهدافها، فالمنهج الوصفي استخدم من أجل وصف جريمة تبييض الأموال وتوضيح خصائصها، كما يمكن المنهج الوصفي من استقراء المواد العلمية التي

تخدم إشكالية البحث، ووظفنا المنهج التحليلي لتحليل النصوص القانونية المرتبطة بموضوع الدراسة، إضافة إلى المنهج المقارن الذي استعملناه لمقارنة بعض التعريفات.

للإحاطة بهذه الإشكالية، فقد ارتأينا تقسيم الدراسة إلى فصلين، حيث جاء (الفصل الأول) بعنوان الإطار المفاهيمي والتقني لجريمة تبييض الأموال في البيئة الرقمية، وقد تناولنا فيه ماهية تبييض الأموال في ظل التحول الرقمي في (المبحث الأول)، ثم خصصنا (المبحث الثاني) للحديث عن الوسائل التقنية المستحدثة في عملية تبييض الأموال، أما الفصل الثاني فقد عنون ب: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية و إشكالات الملاحقة، وقد قسمناه إلى مبحثين اثنين أولها جاء تحت عنوان: الجهود الوطنية والدولية لمكافحة تبييض الأموال في البيئة الرقمية (المبحث الأول)، وتناولنا تحديات الإثبات والملاحقة في جريمة تبييض الأموال في البيئة الرقمية في (المبحث الثاني)، وانهيينا هذه الدراسة بخاتمة أدرجنا فيها النتائج المهمة في هذه الدراسة، وأعقبناها بمجموعة من الاقتراحات.

الفصل الأول

الإطار المفاهيمي والتقني لجريمة

تبييض الأموال في البيئة الرقمية

الفصل الأول

الإطار المفاهيمي والتقني لجريمة تبييض الأموال في البيئة الرقمية

يعد تبييض الأموال في البيئة الرقمية من أخطر الجرائم الاقتصادية التي تهدد الاستقرار الاقتصادي للمجتمعات، فتبييض الأموال هي عملية تحويل الأموال الناتجة عن الأنشطة غير المشروعة إلى أموال تبدو قانونية من خلال سلسلة من العمليات المالية المعقدة، بحيث تساهم في انتشار الفساد وتضخم الاقتصاد غير الرسمي، مما يضعف من قدرة الدول على تحقيق التنمية الاقتصادية المستدامة، وقد ساعد على انتشار هذه الظاهرة سهولة انتقال رؤوس الأموال إلى الدول المختلفة، في ظل تحرير التجارة الدولية، مما آل إلى تزايد حركة تداول أموال المنظمات الإجرامية على المستوى المحلي والدولي، إلا أن التطور التقني زاد من خطورتها وآثارها الاقتصادية ومن أجل توضيح ذلك قمنا بتقسيم هذا الفصل إلى مبحثين حيث عنون (المبحث الأول) ب: الإطار المفاهيمي لجريمة تبييض الأموال في ظل التحول الرقمي، أما (المبحث الثاني) فقد جاء بعنوان: الوسائل التقنية المستحدثة في عمليات التمويه الرقمي.

المبحث الأول

الإطار المفاهيمي لجريمة تبييض الأموال في ظل التحول الرقمي

يشهد العالم في ظل التحول الرقمي تطوراً متسارعاً في أساليب ارتكاب الجرائم المالية وعلى رأسها جريمة تبييض الأموال، حيث يقوم المجرمون بتحويل أو نقل هذه الأموال التي يتحصلون عليها من عمل غير شرعي إلى طرق مشروعة.

ولمعالجة هذا قسمنا هذا المبحث إلى مطلبين فجاء (المطلب الأول) بعنوان: ماهية تبييض الأموال في البيئة الرقمية، أما (المطلب الثاني) فقد عنون ب: مراحل جريمة تبييض الأموال في ظل التحول الرقمي وخصائصها

المطلب الأول

ماهية تبييض الأموال في البيئة الرقمية

قبل أن نتطرق إلى ماهية تبييض الأموال في البيئة الرقمية لابد من الإشارة إلى أن هذه الجريمة تندرج ضمن فئة الجرائم الاقتصادية، الأمر الذي يقتضي بداية بيان مفهوم الجريمة الاقتصادية (الفرع الأول) باعتبارها الإطار العام الذي تنتمي إليه، ثم الانتقال إلى مفهوم جريمة تبييض الأموال في البيئة الرقمية (الفرع الثاني) ومفهوم البيئة الرقمية (الفرع الثالث) من خلال عرض مختلف المفاهيم اللغوية، والاصطلاحية، والقانونية.

الفرع الأول

مفهوم الجريمة الاقتصادية

لا يوجد رأي موحد حول مفهوم الجريمة الاقتصادية، فهناك مفهومان أحدهما واسع (أولا) والآخر محدود (ثانيا).

أولا _ الجريمة الاقتصادية بمفهومها الواسع:

عرفت الجريمة الاقتصادية بمفهومها الواسع بأنها: "كل جريمة تضر أو يحتمل أن تضر بمصلحة اقتصادية أو بالدخل القومي سواء وقعت من الافراد أو من الموظفين أثناء تأدية مهامهم، وسواء وقعت على مال عام او خاص"¹

فالجريمة الاقتصادية بمفهومها الموسع هي: "كل ما يمس الاقتصاد بصفة عامة فتشمل بذلك الجرائم الموجهة ضد الذمة المالية والتي ترتكب أثناء ممارسة النشاط الاقتصادي أو لها ضرر بالنشاط بالاقتصاد الوطني وهذا مثل تزيف النقود والسرقات او الاختلاسات في المنشآت الاقتصادية"²

نستنتج من خلال هذا التعريف أن الجريمة الاقتصادية هي كل جريمة سواء كانت مخالفة أو جنائية سواء كانت مصلحة عامة او خاصة وكانت تمس بالدخل الفردي أو بالدخل الوطني، ويدخل ضمن هذا

¹ محمد خميخ، الطبيعة الخاصة للجريمة الاقتصادية في التشريع الجزائري، مذكرة لنيل شهادة الماجستير في القانون الجنائي والعلوم الجنائية، كلية الحقوق بن عكنون، جامعة الجزائر، 2010-2011، ص12.

² فاضلي سيد علي، التنظيم القانوني للجريمة الاقتصادية وخصوصيتها في التشريع الجزائري، مجلة دفاتر اقتصادية، جامعة المسيلة، الجزائر، المجلد 14، العدد 1، 2023، ص771.

الفصل الأول: الإطار المفاهيمي والتقني لجريمة تبييض الأموال في البيئة الرقمية

التعريف جرائم اختلاس الأموال وجرائم التخريب، والحصول على ربح عن طريق الأضرار بمصلحة الدولة وجرائم الرشوة وغيرها من الجرائم.

ثانياً _ الجريمة الاقتصادية بمفهومها المحدود:

وتعرف بأنها: "مجموعة الجرائم التي تمثل اعتداء على السياسة الاقتصادية والتي تمثل في القانون الاقتصادي للدولة وهو مجموعة النصوص التي تحمي بها سياستها الاقتصادية"¹

فالاتجاه الضيق في تعريف الجريمة الاقتصادية حدد ميدان الجريمة الاقتصادية بعملية المبادلات في إطار السوق، فالجريمة الاقتصادية هي كل فعل أو امتناع يخالف قواعد المنافسة وتحديد الأسعار²

"وقد اعتبر المشرع الفرنسي الجرائم التي تمس أو تضر المؤسسات الخاصة وأموال الأفراد جرائم اقتصادية آخذاً بالمفهوم الاجتماعي الواسع للجرائم الاقتصادية، ويعتبر التعريف الأول هو الراجح في التشريعات الحديثة في الفقه والقضاء الحديثين"³.

يتضح من خلال هذه التعريفات أن الجريمة الاقتصادية بتعريفها الضيق تقتصر على الجرائم الضارة في المال العام وبالتالي فإنه يخرج من هذا التعريف الجرائم الماسة باقتصاديات الأفراد والقطاع الخاص لأن الجرائم الاقتصادية تحمي المال العام وحده أما المال الخاص فتحميه القواعد العامة في قانون العقوبات.

الفرع الثاني

مفهوم جريمة تبييض الأموال في البيئة الرقمية

تعد ظاهرة تبييض الأموال في البيئة الرقمية من الظواهر الخطيرة التي تواجه الكثير من دول العالم لما لها من انعكاسات سلبية على الاقتصاد والمجتمع، وقد تضاربت المفاهيم الفقهية حول ظاهرة تبييض الأموال لحدائتها ونالت حظ كبير من الدراسة والبحث، فتعددت المصطلحات الدالة على عمليات إضفاء الطابع الشرعي على الأموال المحصلة من مصدر غير مشروع، ومصطلح "تبييض الأموال" يدخل ضمنها غير أن المصطلح الأدق هو "غسل الأموال" كما سيأتي تبينه لاحقاً.

ولهذا تطرقنا (أولاً) مفهوم جريمة تبييض الأموال و(ثانياً) إلى أركان جريمة تبييض الأموال

¹ محمود محمود مصطفى، الجرائم الاقتصادية في القانون المقارن، ج1، ط1، مطبعة القاهرة والكتاب الجامعي، مصر، 1979، ص44.

² فاضلي سيد علي، التنظيم القانوني للجريمة الاقتصادية وخصوصيتها في التشريع الجزائري، (مرجع سابق)، ص770.

³ لوني فريدة، القواعد العامة للجرائم الاقتصادية في التشريع الجزائري، مجلة الدراسات الحقوقية، جامعة أكلو محند اولحاج البويرة، الجزائر، المجلد9، العدد2، ديسمبر2022، ص35.

أولاً- مفهوم جريمة تبييض الأموال:

يعد تبييض الأموال من المصطلحات الحديثة نسبياً في مختلف البحوث والدراسات لذا اختلف الراي حول تحديد المقصود بهذا المصطلح بين رجال القانون والفقهاء وامتدت آثاره إلى التشريعات الوطنية والدولية¹

1. تعريف جريمة تبييض الأموال:

لا يوجد تعريف موحد لتبييض الأموال، وذلك لتعدد وجهات النظر والزوايا التي عولجت منها، حيث يمكننا إجراء عدة تعريفات لعملية تبييض الأموال من خلال تقسيمها إلى تعريفات لغوية وأخرى فقهية مقدمة من طرف متخصصين باحثين في ميدان القانون الجنائي والمصرفي وتعريفات قانونية مستخلصة من مختلف النصوص القانونية في هذا الشأن، بالإضافة إلى تعريفات اقتصادية مبنية على معيار وظيفي تجريبي².

أ . تعريف تبييض الأموال لغة:

يفيد مصطلح تبييض أو غسيل أو تطهير في القواميس العربية معنى إزالة الوسخ عن الشيء، أو التطهير من الإثم، واستخدام "الغسل" هنا ليس على بابه وإنما على سبيل المجاز، فإذا كان الغسل للشيء يطهره مما به من أوساخ فغسل الأموال من قبل عصابات الإجرام، المنظم يراد منه إظهاره للغير على أنه مال مباح، ومن مصدر مباح، وأنهم يمارسون أعمالاً مشروعة، فلا يرد على ذهن السلطات ملاحقتهم أو مصادرة تلك الأموال فالجامع المشترك بين المعنيين هو إظهار حسن الشيء

كما يعبر عنها أيضاً بمصطلح "تبييض الأموال" وهو المصطلح الذي اعتمدناه في هذه الدراسة بمعنى اكتساب الأموال³

¹ حميد قطوش، دراسة فعالية منظومة محاربة تبييض الأموال وتمويل الإرهاب في الجزائر، أطروحة مقدمة لنيل شهادة الدكتوراه في

علوم التسيير، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة الجزائر 3، 2018/2019، ص3.

² دليلة جلالية، جريمة تبييض الأموال، ط1، دار المتقف العربي، الجزائر، 2025، ص 13.

³ المرجع نفسه، ص14.

جاء في القاموس الصغير petit Robert أن غسل أو تبييض الأموال هي: "جميع العمليات التي تنطوي على إعطاء النقود والأموال غير المشروعة الوجود القانوني أو الحياة الشرعية باستخدام حيل غير مشروعة أو بارتكاب أفعال غش واحتيال"¹

ب-تعريف جريمة تبييض الأموال قانونا:

تجدر الإشارة إلى أن مفهوم تبييض الأموال من المنظور القانوني فيه اختلاف ما بين الدول، حيث تأخذ بعض الدول بالمفهوم الضيق لتبييض الأموال وتقتصر هذه العمليات على محاولات إخفاء المتحصلات من الإتجار غير المشروع في المخدرات دون بقية الجرائم، فيما تأخذ دول أخرى المفهوم الواسع بحيث تشمل المتحصلات كافة الأعمال الإجرامية²

ولتحديد التعريف القانوني لجريمة تبييض الأموال سوف نتطرق أولا إلى مفهومها في الاتفاقيات والمنظمات والهيئات الدولية، وكذلك في بعض التشريعات الوطنية.

. عرفت الاتفاقيات والمنظمات الدولية: عرفت اتفاقية الأمم المتحدة لمكافحة الاتجار غير المشروع بالمخدرات والمؤثرات العقلية 1988:

نصت المادة (3) على اتخاذ التدابير المتعلقة بتجريم الأفعال التالية: "تحويل الأموال أو نقلها مع العلم بأنها مستمدة من أي جريمة من الجرائم المنصوص عليها في الفقرة الفرعية أ، وكذلك إخفاء أو تمويه حقيقة الأموال أو مصدرها أو مكانها أو طريقة التصرف فيها أو حركتها"³

وبالنظر إلى هذا التعريف نجده ضيق حيث اقتصر على الأموال غير المشروعة المتأتية من جرائم الاتجار غير المشروع بالمخدرات والمؤثرات العقلية.

-عرفها مشروع القانون العربي الإرشادي لمكافحة تبييض الأموال: والذي جاء فيه: "أي فعل يعترف مباشرة أو من خلال وسيط بغية اكتساب أموال أو حقوق أو ممتلكات أيا كان نوعها أو التصرف فيها أو إرادتها أو حفظها في خزانة أو تبادلها أو إيداعها أو ضمانها أو استثمارها أو نقلها أو حيازتها أو تحويلها، مع العلم بأن تلك الأموال أو الحقوق أو الممتلكات متأتية من جريمة أو تمثل عائدات جرمية لغرض

¹ Le nouveau petit robert dictionnaire alphabetique et analogique de la langue française(relie)de Josette Rey ,Debove,Auteur,2005,p502 .

² دليلة جلالية، مرجع سابق، ص18.

³ أمجد سعود القطيفان الخريشة، جريمة غسل الأموال دراسة مقارنة، ط1، دار الثقافة للنشر والتوزيع، الأردن، 2006، ص 26.

الفصل الأول: الإطار المفاهيمي والتقني لجريمة تبييض الأموال في البيئة الرقمية

إخفاء منشأها غير المشروع أو التمويه أو الحيلولة دون اكتشافه، أو لغرض مساعدة أي شخص ضالع في ارتكاب الجرم الأصلي على الإفلات من العقاب القانونية لأفعاله¹

-عرفتها التشريعات: سوف نتعرض لتعريف تبييض الأموال وفقا للتشريع الجزائري وكذا المصري كنماذج قانونية لهذه الدراسة.

-عرفها المشرع الجزائري في المادة 2 من القانون 05/01 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما المعدل والمتمم وذلك على النحو التالي يعتبر تبييضا للأموال²:

. تحويل الأموال أو نقلها مع علم الفاعل بأنها عائدات مباشرة أو غير المباشرة من جريمة بغرض إخفاء أو تمويه المصدر غير المشروع لتلك الأموال أو مساعدة أي شخص متورط في ارتكاب الجريمة الأصلية التي تحصلت منها هذه الأموال على الإفلات من الآثار القانونية لأفعاله.

. إخفاء أو تمويه الطبيعة الحقيقية للأموال أو مصدرها أو مكانها أو كيفية التصرف فيها أو حركتها أو الحقوق المتعلقة بها مع علم الشخص القائم بذلك وقت تلقيها بأنها تشكل عائدات إجرامية.

. المشاركة في ارتكاب أي من الجرائم المقررة وفقا لهذه المادة أو التواطؤ أو التآمر على ارتكابها ومحاولة ارتكابها والمساعدة والتخريض على ذلك وتسهيله وإسداء المشورة بشأنه.

مما يفيد أن الركن المادي لهذه الجريمة تقوم على إتيان أحد العناصر السالفة ذكرها (تحويل أو نقل أو إخفاء أو تمويه الطبيعة الحقيقية لها أو مصدرها أو مكانها أو كيفية التصرف فيها أو حركتها أو الحقوق المتعلقة بها أو اكتساب الممتلكات أو حيازتها أو استخدامها) أما الركن المعنوي إنما يتجسد في علم الجاني بأن هذه الأموال أو الممتلكات إنما هي عائدات إجرامية ومع ذلك يأتي على إخفاء أو تمويه مصدرها

-عرفها المشرع المصري في المادة الثانية من قانون مكافحة غسل الأموال رقم 154 بأنه: "كل سلوك ينطوي على اكتساب أموال أو حيازتها أو التصرف فيها أو إدارتها أو حفظها أو استبدالها أو إيداعها أو ضمانها أو استثمارها أو نقلها أو تحويلها أو التلاعب في قيمتها إذا كانت متحصلة من الجرائم المنصوص عليها في المادة (2) من هذا القانون مع العلم بذلك متى كان القصد من هذا السلوك إخفاء المال أو تمويه

¹ علي العريان، عمليات غسل الأموال وآليات مكافحتها، د ط، دار الجامعية الجديدة للنشر، الإسكندرية، مصر، 2009، ص32.

² القانون رقم 25 - 10 المؤرخ في 24 جويلية 2025 المعدل للقانون 01-05، المادة 2، المؤرخ في 27 ذي الحجة عام 1425 هـ الموافق لـ 06 فبراير 2005 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحته، ج ر، العدد 48.

الفصل الأول: الإطار المفاهيمي والتقني لجريمة تبييض الأموال في البيئة الرقمية

طبيعته أو مصدره أو مكانه أو صاحبه أو صاحب الحق فيه أو تغيير حقيقته أو الحيلولة دون اكتشاف ذلك أو عرقلة التوصل إلى شخص من ارتكب الجريمة المتحصل منها المال"¹

ج-التعريف الفقهي:

سوف نركز على تعريف جريمة تبييض الأموال لدى جملة من الفقهاء سواء العربيين أو الغربيين كالآتي:

عرفت بأنها: "كل فعل يقصد به تمويه أو إخفاء مصدر الأموال أو المداخل الناتجة بصورة مباشرة أو غير مباشرة عن ارتكاب إحدى الجرائم"²

ويوجد تعريف آخر وهو: "إخفاء حقيقة الأموال المستمدة من طريق غير مشروع عن طريق القيام بتصديرها، أو إيداعها في مصاريف دول أخرى أو نقل إيداعها، أو توظيفها أو استثمارها في أنشطة مشروعة للإفلات بها من الضبط والمصادرة وإظهارها كما لو كانت مستمدة من مصادر مشروعة، وسواء كان الإيداع أو التمويه أو النقل أو التحويل أو التوظيف أو الاستثمار قد تم في دول متقدمة أو في دول نامية"³ وقيل أيضا أن جريمة تبييض الأموال هي تلك: "النشاطات غير المشروعة التي تهدف إلى إخفاء أو تمويه الأموال الناتجة عن الجريمة المنظمة"⁴.

نخلص إلى أن هذه التعاريف قد ركزت على فعل الإخفاء أو التمويه الذي ينصب على مصدر المال محل الغسل، في حين هناك جانب آخر من الفقه يركز على أن فعل الإخفاء ينصب على حقيقة الأموال غير المشروعة.

¹ القانون رقم 154 لسنة 2022، المادة 2، الصادرة بتاريخ 15 يونيو 2022، جمهورية مصر العربية، المعدل لقانون رقم 80،

2002 بشأن مكافحة غسل الأموال، ج ر، العدد 23 مكرر

² عادل عكروم، جريمة تبييض الأموال دراسة مقارنة، جامعة سعد دحلب، د ع، د ت ن، ص 128.

³ المرجع نفسه، ص 129.

⁴ المرجع نفسه، ص 129.

ثانيا . أركان جريمة تبييض الأموال

تقوم جريمة غسل الأموال في البيئة الرقمية على أركان أساسية ثلاثة والتي لا تحقق بدونها قانونا وهي الركن القانوني أو الشرعي وهو: " نص التجريم الذي يجرم الفعل ويعاقب عليه"¹، وركن مادي الذي يمثل ماديات الجريمة، وركن معنوي وهو الحالة النفسية للجاني وقت ارتكاب الجريمة².

1- الركن الشرعي:

تنص المادة الأولى من قانون العقوبات أن: "لا جريمة ولا عقوبة ولا تدابير أمن بغير قانون"³، ولكن هذا القانون جاء خالياً من أي نص يجرم عملية تبييض الأموال عند صدوره سنة 1966، لأن هذه الجريمة حديثة استفحلت فقط في العقدين الأخيرين من القرن، ومن أجل مواكبة التطورات الاقتصادية والاجتماعية والسياسية فقد بادرت الجزائر للمصادقة على اتفاقية الأمم المتحدة لمكافحة الاتجار بالمخدرات والمؤثرات العقلية بفيينا بتاريخ 20/12/1988، والتي دخلت حيز التنفيذ في 11/11/1990 وذلك بموجب المرسوم رقم 41/95 المؤرخ في 28 يناير 1995 المتضمن المصادقة بتحفظ على الاتفاقية⁴

كما صادقت الجزائر على اتفاقية قمع تمويل الإرهاب لسنة 1995، وذلك بموجب مرسوم رئاسي رقم 445/200 المؤرخ في 23/12/2000، اتفاقية الجريمة المنظمة عبر الوطنية لسنة 2000 بموجب مرسوم رئاسي رقم 55/02 المؤرخ في 25/02/2002 ونجد أن المشرع الجزائري قد أصدر عدة نصوص قانونية لها علاقة بجريمة تبييض الأموال وذلك في الأمر رقم 22/96 المؤرخ في 09/07/1996 المتعلق بقمع مخالفة التشريع والتنظيم الخاصين بالصرف وحركة رؤوس الأموال من وإلى الخارج، حيث أن المادة الأولى منه تعتبر مخالفة التشريع والتنظيم النقدي الخاصين بالصرف وحركة رؤوس الأموال من وإلى الخارج بأي وسيلة⁵:

¹ سرارية عيشوش، جريمة تبييض الأموال وفق التشريع الجزائري، مذكرة مكملة من متطلبات شهادة الماستر في الحقوق، كلية

الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2015/2016، ص18.

² خديجة خلوفي، فريدة لوني، أركان جريمة تبييض الأموال في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية جامعة محمد بوضياف المسيلة، المجلد2، العدد8، 2017، ص600.

³ الأمر رقم 66-156، المادة 1، المؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات، ج ر، العدد49، 1966.

⁴ خديجة خلوفي، فريد لوني، مرجع سابق، ص 600.

⁵ الأمر رقم 22/96 ، المادة 1، المؤرخ في 09/07/1996، المتعلق بقمع مخالفة التشريع والتنظيم الخاصين بالصرف وحركة رؤوس الأموال من وإلى الخارج، ج ر، العدد43، 1996.

. تصريح كاذب

- عدم مراعاة التزامات التصريح

. عدم استرداد الأموال إلى الوطن

. عدم مراعاة الإجراءات المنصوص عليها والشكليات المطلوبة

. عدم الحصول على التراخيص المشتركة

- عدم الاستجابة للشروط المفترضة بهذه التراخيص...

كما أن المادة الرابعة منه أشارت إلى العمليات المتعلقة بالنقود والأوراق المزيفة، والتي تشكل مخالفة لهذا التنظيم، وأصدر المشرع الجزائري المرسوم التنفيذي رقم 22.36 المؤرخ في 4 جانفي 2022 المتضمن إنشاء خلية معالجة الاستعلام المالي وتنظيمها وسيرها، حيث تنص المادة 04 منه على أنه: "تكلف الخلية بمكافحة تمويل الإرهاب وتبييض الأموال وتتولى بهذه الصفة المهام الآتية على الخصوص:

. تستلزم تصريحات الاشتباه المتعلقة بكل عمليات تمويل الإرهاب وتبييض الأموال التي ترسلها إليها الهيئات والأشخاص الذين يعينهم القانون..."¹

والجدير بالملاحظة حول هذه الترسنة القانونية، هو أن المشرع الجزائري لم يستعمل صراحة مصطلح "التبييض" ولكن استعمل عدة ألفاظ تدل عليه².

2- الركن المادي

نعني بالركن المادي لجريمة تبييض الأموال المظهر الخارجي للجريمة والذي به يتحقق الاعتداء على المصلحة العامة والخاصة ويتمثل في كل فعل يساهم في إخفاء أو تمويل مصدر الأموال والمداخل الناتجة سواء بصورة مباشرة أو غير مباشرة عن جميع الجرائم³.

¹ المرسوم التنفيذي، رقم 22.36، المؤرخ في 4 جانفي 2022، المتضمن إنشاء خلية معالجة الاستعلام المالي وتنظيمها وسيرها

المادة 04، المتضمن إنشاء خلية معالجة الاستعلام المالي وتنظيمها وعملها، ج ر، العدد 3، 2022.

² خديجة خلوفي، فريدة لوني، مرجع سابق، ص 602.

³ المرجع نفسه، ص 603.

أ. السلوك الاجرامي:

تتعدد أنماط النشاط في الركن المادي لجريمة تبييض الأموال كون التشريعات المختلفة لم تتفق على صور بعينها، فاتفاقية فيينا وكذلك المشرع الجزائري في المادة 389 مكرر من قانون العقوبات حدد ثلاث صور لعمليات تبييض الأموال وهي:

. تحويل الأموال

. إخفاء أو تمويه الطبيعة الحقيقية للأموال

. حيازة أو اكتساب أو استخدام هذه الأموال

. **تحويل الأموال ونقلها:** نعني بتحويل الأموال إجراء عمليات مصرفية أو غير مصرفية الغرض منها تحويل الأموال المتحصلة من جريمة في شكل آخر، أي الغرض منها إخفاء أو تمويه مصدرها كتحويل النقود الفذرة المتحصلة عن تجارة المخدرات مثلاً إلى مجوهرات أو ذهب ثم القيام ببيعها مقابل عملات أجنبية كالدولار، وقد يتم تحويل الأموال من عملة وطنية إلى عملة أجنبية خاصة في الدول التي لا تفرض أية قيود على هذه التحويلات¹.

- **إخفاء أو تمويه الطبيعة الحقيقية للأموال:** أي إخفاء مصدر الأموال غير المشروعة، أي الحيلولة دون كشف الحقيقة في أمر الجريمة الأصلية التي تحصلت منها الأموال محل الإخفاء.

والإخفاء هو كل عمل من شأنه منع الحقيقة عن المصدر غير المشروع، سواء كان هذا الإخفاء مادياً أو علنياً، كما لا يهم سبب الإخفاء حتى ولو كان بطريقة مشروعة ك شراء الشيء، أو الادعاء بالسرقة، أو اكتساب الأموال غير المشروعة بطريق الهبة.

أما فعل التمويه فيقصد به اصطناع مصدر مشروع غير حقيقي للأموال غير المشروعة كإدخال هذه الأموال في الأرباح الناتجة عن إحدى الشركات القانونية وتظهير هذه الأموال كأرباح للشركة، ويتمثل محل الإخفاء أو التمويه في حقيقة الأموال أو مصدرها أو مكانها أو طريقة التصرف فيها أو حركتها أو الحقوق المتعلقة بها أو ملكيتها.

- **حيازة أو اكتساب الأموال:** وهذه الحالة تنطبق بالأخص على البنوك والمؤسسات المالية، حيث توضع الودائع والمبالغ المالية غير المشروعة في هذه المؤسسات، وهي على علم بالمصدر غير المشروع للأموال

¹ خديجة خلوفي، فريدة لوني، مرجع سابق، ص 603

الفصل الأول: الإطار المفاهيمي والتقني لجريمة تبييض الأموال في البيئة الرقمية

سواء كان هذا الإيداع في شكل رصيد أو فتح حساب أو في شكل أمانة، ولكن يبنى علم المؤسسة المالية بالمصدر المفترض، ومن أجل تجنب هذا الافتراض عملت أنظمة الصرف في التشريع المقارن والتي تجرم عملية تبييض الأموال، إلى وضع ميكانيزمات تقنية من أجل تبرئة ذمة المؤسسات المالية، وذلك عن طريق تبليغها للسلطات المختصة عن كل رصيد بنكي يتجاوز مبلغ معين حسب متوسط قدرة الادخار للمواطن العادي، كما أنه هناك ميكانيزم آخر وهو تبليغ البنك عن كل مبلغ مالي يدخل لأحد الأرصدة بدون أن يكون مبرراً بشكل كاف.

غير أن الواقع أثبت عدم نجاعة هذه الطرق لأنه يضع صاحب الحساب دوماً في عبء تقديم دليل على مشروعية أمواله، في حين يفترض أن تكون ذمة الشخص خالية من أي عبء وعلى من يدعي خلاف ذلك إقامة الدليل وفقاً لطرق الإثبات

لقد ميزت اتفاقية فيينا لسنة 1988 بين ثلاث أنواع من السلوكيات واعتبرت الإقدام على ارتكاب أي نوع منها جريمة، وتتمثل هذه الأفعال في:

-حيازة الأموال المتحصل عليها من الاتجار بالمخدرات:

إن مجرد قبول الفاعل سواء كان شخصاً طبيعياً أو معنوياً، استلام هذه الأموال من مبيض الأموال والاحتفاظ بها لديه أو في حسابه الخاص بالبنك، يعد جانباً لأنه يعلم بالمصدر غير المشروع لهذه الأموال¹

-اكتساب الأموال المتحصل عليها من الجرائم:

يشكل فساد ذمم بعض الأشخاص من جراء الإغراءات المالية التي تمنح لهم، مقابل تعاونهم في عمليات الإخفاء أو التمويه عن المحاصيل غير المشروعة للأموال غير المشروعة، كإحدى أبرز أهم النتائج السلبية التي تفرزها التجارة غير المشروعة بالمخدرات.

ويتم ذلك من خلال منح هؤلاء عمولات مالية عن كل مبلغ يتم غسيله، أو اللجوء إلى دفع الرشاوي ومنح الهدايا إلى الأشخاص الذين يظهرون استعدادات لمساعدتهم، سواء كانوا موظفون في قطاع الدولة كالموظفون في الجمارك، والبنوك، أو الموظفون في القطاع الخاص كالمحامين، المحاسبين... الخ وهي فئات ترتكب جريمة قبول الرشوة، وهي منفصلة عن جريمة تمويه حقيقة الأموال التي تحصل عليها شخص آخر.

¹ خديجة خلوفي، فريدة لوني، مرجع سابق، ص ص 603-604.

الفصل الأول: الإطار المفاهيمي والتقني لجريمة تبييض الأموال في البيئة الرقمية

- استخدام الأموال المتحصلة من الجرائم: لقد وسعت اتفاقية فيينا 1988 من دائرة التجريم عندما اعتبرت نشاط استخدام واستثمار هذه الأموال من قبل الجرائم، ولكن بشرط علم المستثمر بحقيقة هذه الأموال في نشاط مشروع وغير مشروع، ولكن إذا لم يكن المستثمر على علم بمصدر هذه الأموال فإنه لا يعد مرتكباً لأية جريمة حسب قانون العقوبات¹.

إن جريمة تبييض الأموال هي جريمة تهدف إلى إضفاء طابع الشرعية على الأموال ذات المصدر الإجرامي، وهي بذلك جريمة تبعية سبقتها جريمة أصلية أو أولية، تكون مصدر الأموال غير المشروعة المراد تبييضها مثل جريمة التهريب، الاتجار بالأسلحة، الاتجار بالمخدرات... الخ.

ب . الجريمة الأصلية أو الأولية: تعد جريمة تبييض الأموال جريمة تبعية، ويفترض وقوع جريمة أصلية سابقة وهي مصدر الأموال القذرة.

إن المتحصلات الناتجة عن نشاط إجرامي أو مصدر غير مشروع وغير قانوني، هي أية أموال مستمدة أو حصل عليها الجاني بطريق مباشر أو غير مباشر من ارتكاب جريمة من الجرائم المعاقب عليها قانوناً ولقد تباينت القوانين حول تعريف الأموال القذرة، بأنها متحصلة من جرائم حددها المشرع في بعض الدول وتغاضى عنها في دول أخرى.

وبالتالي يمكن تحديد الجريمة الأولى بإحدى الطرق التالية:

الطريقة الأولى: عدم تحديد الجرائم بصفة عامة، بحيث يتسع نطاق الجرائم الأصلية ليشمل كل الأفعال المجرمة قانوناً .

الطريقة الثانية: يتم حصر الجرائم الأصلية في إطار محدود .

الطريقة الثالثة: وهي تجمع بين الطريقتين السابقتين مثل النص على اعتبار الجنايات مصدراً للمال غير المشروع، ثم ذكر بعض الجناح على سبيل الحصر² .

إذا كانت اتفاقية فيينا لسنة 1988 قد حصرت الجرائم الأصلية المرتبطة بتبييض الأموال في جرائم المخدرات، فإن المشرع الجزائري اتجه نحو توسيع نطاق التجريم بصورة تدريجية، حيث لم يقتصر على الجرائم التقليدية، بل وسّع الحماية القانونية لتشمل صوراً حديثة للجريمة المالية المرتبطة بالبيئة الرقمية،

¹ خديجة خلوفي، فريدة لوني، مرجع سابق، ص 604.

² المرجع نفسه، ص 605.

الفصل الأول: الإطار المفاهيمي والتقني لجريمة تبييض الأموال في البيئة الرقمية

لاسيما من خلال القانون رقم 10-25 الذي جرم التعامل بالأصول الافتراضية والمنصات الرقمية المرتبطة بها¹

ج - الشروع وإتمام عملية التبييض: ونعني بها القيام بالسلوك المادي الذي بمقتضاه تكتسي العائدات الإجرامية صفة مصدر مشروع، يتيح لحائزها التصرف بكل حرية .

ولقد نصت المادة 04 من قانون 01-05 المعدل على تعريف الأموال محل الجريمة على أنه: "أي نوع من الممتلكات أو الأموال من أي طبيعة كانت بما فيها الموارد الاقتصادية والقيم المالية الافتراضية المادية وغير المادية المنقولة وغير المنقولة التي يحصل عليها باي وسيلة كانت مباشرة أو غير مباشرة..²"

وبالتالي فإن المشرع الجزائري قد اعتبر المال محل جريمة تبييض الأموال بأنه يشمل في نطاقه كافة الأموال والعائدات الناتجة عن الجريمة الأصلية بغض النظر عن نوعها وأياً كانت طبيعتها³.

وقد تعزز هذا التوجه أكثر بعد التعديلات الحديثة التي جاء بها القانون رقم 10-25، حيث وسّع المشرع الجزائري نطاق الأموال محل الجريمة ليشمل الأصول الافتراضية والقيم الرقمية القابلة للتداول أو التحويل إلكترونياً، وذلك في إطار مواجهة الأساليب المستحدثة لتبييض الأموال في البيئة الرقمية⁴

3. الركن المعنوي:

الركن المعنوي هو القصد الجنائي، فجريمة تبييض الأموال الإلكترونية من الجرائم العمدية التي تقوم على القصد الجنائي العام والقصد الجنائي الخاص⁵ ويتحقق الركن المعنوي في معظم الجرائم بتوافر القصد العام الذي يركز على عنصرى العلم والإرادة، إلا أنه هناك بعض الجرائم التي لا بد فيها من القصد الخاص

¹ القانون رقم 10-25 المؤرخ في 24 جويلية 2025، المعدل والمتمم للقانون رقم 01-05 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، ج ر، العدد 48، 2025.

² القانون رقم 01-05 المادة 4، المؤرخ في 6 فبراير 2005، المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، ج ر، العدد 11، 2005.

³ خديجة خلوفي، فريدة لوني، مرجع سابق، ص 606.

⁴ القانون رقم 10-25 المؤرخ في 24 جويلية 2025، المعدل والمتمم للقانون رقم 01-05 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، ج ر، العدد 48، 2025.

⁵ عبد الرحمان خلفي، المسؤولية الجنائية للأشخاص المعنوية في جرائم تبييض الأموال، المجلة الأكاديمية للبحث القانوني، جامعة عبد الرحمان ميرة، بجاية، العدد 2، 2011، ص 34.

الفصل الأول: الإطار المفاهيمي والتقني لجريمة تبييض الأموال في البيئة الرقمية

لاكتمال عناصرها، وفي جرائم تبييض الأموال التي تعتبر جرائم عمدية يجب أن يتوافر فيها القصد العام والخاص¹

فالمشرع الجزائري يأخذ بالقصد العام والخاص في جريمة تبييض الأموال، فالعام يتمثل في عنصري العلم والإرادة، والخاص يظهر من خلال المادة 389 مكرر من قانون العقوبات والمادة 02 من قانون 01/05 المعدل المتعلق بتبييض الأموال.

أ. **القصد العام لجريمة تبييض الأموال**: يقوم القصد العام لجريمة تبييض الأموال على عنصري العلم والإرادة، العلم بالمصدر غير المشروع للأموال أي العلم بالوقائع، إذ يجب أن يحاط علم الجاني عند ارتكابه للنشاط بكل الوقائع التي يترتب على توافرها قيام الجريمة، فجد اتفاقية فيينا لسنة 1988 في المادة 03 تؤكد على اشتراط عنصر العلم عند تعدادها لصور السلوك، حيث قررت في الفقرة الأولى منها حين نصت على صورة تحويل الأموال أو نقلها مع العلم بأنها مستمرة في جريمة، وطبيعة العلم يجب أن يكون يقيناً ولا يكفي الظن أو الاعتقاد بأن مصدر الأموال غير مشروع.

بالرجوع إلى المشرع الجزائري نجد أنه قد أشار في نص المادة 389 مكرر الفقرة أ وب من قانون العقوبات، إلى علم الفاعل والإرادة كجوهر للقصد الجنائي العام، كذلك لأنه في جريمة تبييض الأموال يتطلب توافر الإرادة لدى الجاني لارتكاب الفعل المعاقب عليه وتحقيق النتيجة المطلوبة، أي تتجه نية الفاعل إلى تحقيق نتيجة إجرامية على أن تكون هذه الإرادة حرة وواعية.

توجد صعوبات جمة لاستخلاص النية الإجرامية والتحقق من توافرها في بعض حالات جريمة تبييض الأموال، لا سيما في حالة قبول إيداع أو تحويل الأموال غير المشروعة حيث العمليات المصرفية أصبحت تتم وفقاً لآليات وأساليب متطورة.

ولكن إذا شاب هذه الإرادة عيب فإنه ينتفي الركن المعنوي بانقضاء الإرادة وقد تنتفي المسؤولية الجنائية للفاعل، غير أنه لا يمكن الاحتجاج بالإكراه الأدبي أو تنفيذ أوامر الرؤساء لنفي الإرادة إلا إذا انتفى حسن النية من قبل، بإيداع أو تحويل الأموال غير المشروعة أو بتوافر العلم بعدم مشروعية ما يقوم به²

ب. **القصد الخاص لجريمة تبييض الأموال**: لم يقتصر المشرع الجزائري على القصد العام في جريمة تبييض الأموال وإنما اشترط القصد الخاص وهو ما يستنتج من المادة 02/ من قانون 01/05 المعدل التي

¹ خديجة خلوفي، فريدة لوني، مرجع سابق، ص 606.

² المرجع نفسه، ص 607.

الفصل الأول: الإطار المفاهيمي والتقني لجريمة تبييض الأموال في البيئة الرقمية

تنص على: "تحويل الأموال ونقلها مع علم الفاعل أنها عائدات مباشرة أو غي مباشرة من جريمة بغرض إخفاء وتمويه المصدر غير المشروع لتلك الأموال، أو مساعدة أي شخص متورط في ارتكاب الجريمة الأصلية التي حصلت منها الأموال على الإفلات من الآثار القانونية لأفعاله"¹ فالقصد الخاص هو انصراف نية الجاني نحو تحقيق غاية أو غرض معين، ويدفعه لارتكاب الفعل باعث معين لتحقيق نتيجة غير شرعية.

الفرع الثالث

مفهوم البيئة الرقمية

البيئة الرقمية هي البيئة المتاحة على شبكة الأنترنت، والتي يجري تناول المعلومات من خلالها في شكل رقمي عن طريق استخدام وسائل اتصال جديدة تتيح الوصول المباشر والكامل للمعلومات²

أو هي بيئة اتصالات متكاملة حيث تتواصل الأجهزة الرقمية وتدير المحتوى والأنشطة داخلها يعتمد المفهوم على أنظمة الإلكترونيات الرقمية التي يتم دمجها وتنفيذها من أجل مجتمع عالمي، وتشتمل المكونات الرئيسية للبيئة الرقمية بشكل عام مواقع الويب والخوادم السحابية ومحركات البحث ومنافذ الوسائط الاجتماعية وتطبيقات الأجهزة المحمولة والصوت والفيديو والموارد المستندة إلى الويب³

كما تعرف أيضا على "أنها مجموعة من المفاهيم الحديثة مثل: البحث بالاتصال المباشر، النشر الإلكتروني، قواعد البيانات على أقراص مدمجة، الفهارس الآلية، شبكة المعلومات فائقة السرعة متمثلة في شبكة الأنترنت..."⁴

¹ القانون رقم 05-01 المؤرخ في 6 فبراير 2005، المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتها، ج ر، العدد 11، 2005.

² حسام منصور، الإشهار في البيئة الرقمية مفاهيم أساسية، مجلة التمكين الاجتماعي، جامعة عمار ثلجي، الاغواط، المجلد 4 العدد 2، جوان 2022، ص 61.

³ نجا فتور، عادل شيهب، البيئة الرقمية للتعليم عن بعد في الجامعة الجزائرية قراءة في التحديات والانعكاسات من وجهة نظر الأساتذة والطلبة في جامعة جيجل، مجلة دراسات اقتصادية، جامعة زيان عاشور، الجلفة، المجلد 17، العدد 3، 2023، ص 663.

⁴ نجا فتور، عادل شيهب، مرجع سابق، ص 663.

الفصل الأول: الإطار المفاهيمي والتقني لجريمة تبييض الأموال في البيئة الرقمية

كما عرفت بأنها "مجموعة تقنيات وأدوات إلكترونية وشبكات تعلم شخصية تتيح الوصول إلى المعلومات والموارد بغض النظر عن نوعها وحجمها تتغير فيها المعلومات بسرعة، وفيها العديد من الأدوات التي تتاح للتعامل مع البيانات الواسعة والمتنامية وتسمح بإنشاء شبكات تعلم شخصية"¹

كما وقد عرفت أيضا بأنها: "مجموعة من العناصر ذات المهام والاختصاصات المتفاوتة يتفاعل الإنسان معها في مختلف المؤسسات عبر تطبيق التكنولوجيا الجديدة وتعد شبكة الأنترنت البيئة الأساسية والمناسبة لاحتضان وإتاحة الدخول إلى المعلومات الرقمية، بحيث توفر مصادر المعلومات والوسائط الرقمية المخزنة في قواعد المعلومات وتمكن الباحث من الحصول على أوعية ومصادر المعلومات في أي وقت ومن أي مكان".²

بناء على ما تم ذكره، نعرف البيئة الرقمية على أنها: عبارة عن مجموعة من الخدمات توفرها شبكة الأنترنت وجميع تكنولوجيا المعلومات والاتصال التي تلتحق بها والتي تمكن من الوصول للمعلومات بسرعة فائقة وبشكل كامل كما تقدم خدمة استرجاع المعلومات والتقنيات المستخدمة من قبل الباحثين والخبراء.

المطلب الثاني

مراحل جريمة تبييض الأموال في ظل التحول الرقمي وخصائصها

تعتبر عملية تبييض الأموال عملية ديناميكية تتم على ثلاث مراحل، ففي المرحلة الأولى يتم فصل الأموال عن الجريمة، وفي المرحلة الثانية يتم محو كل آثار الجريمة لتمويه الرقابة، أما في المرحلة الثالثة فإن صاحب هذه الأموال يحاول استرجاعها مهما كانت الطرق المستعملة وبدون إحداث أية شبهة تدل على عدم شرعية تلك الأموال، كما أنها تتسم هذه الجريمة بخصائص وسمات تجعل من مكافحتها تحديا كبيرا للسلطات والجهات الرقابية.

ولمعالجة هذا سنتطرق في هذا المطلب إلى فرعين اثنين: فقد جاء (الفرع الأول) بعنوان: مراحل جريمة تبييض الأموال، أما (الفرع الثاني) فقد كان بعنوان: خصائص جريمة تبييض الأموال في البيئة الرقمية.

¹ نجاة فتور، عادل شهيب، ص 663.

² ناجي بولمناخر، البحث العلمي في ظل البيئة الرقمية: تحديات الواقع وأفاق المستقبل، مجلة دفاتر المتوسط، جامعة باجي مختار، عنابة، المجلد 6، العدد 2، ديسمبر 2021، ص 112.

الفرع الأول

مراحل جريمة تبييض الأموال

تتم جريمة تبييض الأموال غير المشروعة من خلال عمليات معقدة تتم عبر ثلاث مراحل أساسية وهي: (أولا) مرحلة الإيداع وهي المرحلة الأولى يتم فيها إدخال الأموال في الدورة المالية، أما في المرحلة الثانية يتم إخفاء مصدر الأموال وهي ما يسمى بمرحلة التمويه (ثانيا)، وفي المرحلة الأخيرة، وهي مرحلة الدمج يحصل شرعنة للأموال أو توفير الغطاء القانوني لها (ثالثا) ¹

أولا . مرحلة الإيداع:

وهي مرحلة الإيداع أو التوظيف أو الإحلال تشير إلى أنها تقتضي التخلي المادي عن النفوذ المتحصلة من النشاط الإجرامي، أي النشاط غير المشروع بهدف إبعاد الشبهة عن مصدرها، ويتم ذلك في الغالب بأسلوب بسيط عن طريق توظيف الأموال المشبوهة في البنوك، أو في غيرها من المؤسسات المالية سواء في داخل البلاد أو خارجها وسواء بطريق فتح الحسابات أو الودائع أو شراء أوراق مالية... الخ، وفي خلال هذه المرحلة قد يتحقق تنظيف الأموال المشبوهة بتوظيفها داخل المؤسسات المالية، وذلك إما بتزوير بعض المستندات أو إخفاء بعضها أو بتواطؤ بعض موظفي البنك ، وفي البلدان التي تشترط الإبلاغ عن المعاملات النقدية التي تصل مبلغا معينا والتي من بينها قانون العقوبات الفرنسي الذي يشترط على المصرف إبلاغ السلطات المختصة بالتحويلات النقدية التي تكون قيمتها 150 ألف فرنك فرنسي فاكثر، فإن الإيداع في هذه الحالة يتم من خلال إجراء عدد كبير من المعاملات الصغيرة لتفادي الوصول إلى المبلغ المحدد والذي يخضع لقوانين مراقبة النقد الإلزامية، وتشمل الوسائل المستعملة أنواع مختلفة كالودائع المصرفية والأدوات النقدية والمعادن الثمينة والسيارات الفخمة، والتحف الفنية والعقارات، وتعتبر هذه المرحلة من أكثر المراحل أهمية لأنه يتوقف عليها نجاح جريمة تبييض الأموال، وكذلك بالنظر للتعقيدات المعتمدة في إطارها. ²

نستنتج من خلال هذه المرحلة أنه يتم جمع الأموال غير المشروعة وإدخالها في البنوك لإبعاد كل الشبهات وحماية هذه الأموال من المراقبة كما أن هذه المرحلة من أخطر مراحل تبييض الأموال.

¹ نادر عبد العزيز شافي، تبييض الأموال دراسة مقارنة، منشورات حلبي الحقوقية، 2001، ص 117.

² عادل عكروم، مرجع سابق، ص ص 135-136.

ثانيا - مرحلة التمويه:

مرحلة التمويه كما يطلق عليها أيضا بمرحلة التعتيم أو التغطية¹، حيث أنه وبعد قطع الصلة بين الأموال القذرة ومصدرها الغير المشروع، ووضعها في إطار دائرة النظام المالي ينتقل بعد ذلك إلى الخطوة الثانية والمعروفة بمرحلة التمويه وتتم عن طريق إجراء سلسلة من العمليات المالية والمصرفية وغير المصرفية المتتالية تهدف إلى إخفاء معالم مصدر المال، وإبعاده قدر الإمكان عن إمكانية تتبع مصدره الحقيقي، والواقع إذا نجح المال في تخطي المرحلة الأولى فإن الكشف عنه في هذه المرحلة يكون أكثر صعوبة، ومن امثلة التمويه هناك إعادة بيع أو تصدير رأس المال، الذي يتم الحصول عليه في المرحلة الأولى ومقابل البيع أو الشيء المصدر يأخذ صورة دفع نقدي، وهو ما يجعل شخصية المشتري أكثر وضوحا ودون خوف، كما يجعل رأس المال أكثر مرونة في الحركة، كما أنه ومن خلال هذه المرحلة يمكن أن تنتقل الأموال القذرة من دولة إلى أخرى أقل صرامة في التعامل المالي، والتي تركز على السرية المصرفية في التعاملات المصرفية من أجل إخفاء مصدرها الحقيقي مما يجعلها تتصف بالطابع الدولي.²

وخلاصة القول تعتبر مرحلة التمويه المرحلة الأكثر تعقيدا في عملية غسل الأموال، حيث يعتمد المجرمون على إخفاء أثر الأموال غير المشروعة عبر شبكة من التحويلات المعقدة والشركات الوهمية والمنتجات المالية المتقدمة.

ثالثا - مرحلة الدمج:

تعد مرحلة الدمج أو الإدماج أو التكامل أو العصر نسبة إلى المرحلة النهائية من غسل الثياب: وهي المرحلة النهائية والأكثر علانية في عمليات غسل الأموال، ومن شأنها إضفاء صفة المشروعية على الأموال المغسولة ذات الأصل غير المشروع إذ تظهر وقد اندمجت في النظام المالي الشرعي، حيث بلغت من الأمان ما يكفي لاستثمارها بحرية في أية أنشطة أو أصول أخرى غير مشبوهة دون خشية المطاردة والمحاسبة والمصادرة، ومن أكثر الاستثمارات المشروعة سهولة في وقتنا المعاصر اللجوء إلى المضاربة في الأسواق المالية المنتشرة في جميع أنحاء العالم، ويستفاد فيها من الثروة الاتصالية الحديثة من خلال الانترنت حيث تنتقل الملايير من بلد إلى آخر في دقائق، إضافة إلى التسهيلات الائتمانية (القروض)،

¹ دريس باخويا، أحكام مكافحة جريمة تبييض الأموال في التشريع الجزائري، مجلة جامعة أدرار، العدد6، جوان 2016، ص224.

² زيغام أبو القاسم، الآليات الدولية والوطنية لمكافحة جريمة تبييض الأموال، مجلة القانون الدولي والتنمية، جامعة عبد الحميد ابن باديس، مستغانم، العدد5، 2016، ص157.

الفصل الأول: الإطار المفاهيمي والتقني لجريمة تبييض الأموال في البيئة الرقمية

وفتح الاعتمادات المستندية اللازمة للقيام بعمليات الاستيراد و التصدير وفتح حسابات الجارية أو بيع وشراء العقارات بواسطة شركة غطاء SHELL تشتري وتبيع، ويذكر أن الأموال الملوثة لا تعود كلها إلى اوطانها بعد الغسل فالجزء الذي لا يعود لا يأتي في شكل نقدي، بل مستترا في شكل سلعي أو خدمي أو عن طريق طرف ثالث قد يكون غيره الذي أسهم في تهريبه من داخل الاقتصاد أي خروج هذه الأموال يشكل خسارة صافية للاقتصاد القومي.¹

نستنتج أن في هذه المرحلة تصبح الأموال جاهزة للاستخدام في الأنشطة الاقتصادية اليومية دون إثارة الشبهات مما يتيح للمجرمين الاستفادة منها وكأنها أرباح مشروعة، وهي الهدف النهائي من عمليات غسل الأموال.

الفرع الثاني

خصائص جريمة تبييض الأموال في البيئة الرقمية

تعد جريمة غسل الأموال من أكثر الجرائم الاقتصادية تعقيدا وتأثيرا على الاقتصاد العالمي، حيث تتسم بخصائص وسمات تجعل من مكافحتها تحديا كبيرا للسلطات والجهات الرقابية² ، ولهذا سنعالج في هذا الفرع خصائص جريمة تبييض الأموال جريمة غسل الأموال جريمة تبعية (أولا) جريمة غسل الأموال جريمة اقتصادية (ثانيا) جريمة تبييض الأموال جريمة منظمة وعابرة للحدود (ثالثا) عمليات غسيل الأموال عملية مصرفية (رابعا).

تتسم جريمة غسل الأموال بخصائص وهي على النحو التالي:

أولا: جريمة غسل الأموال جريمة تبعية

وهي تبعية لكونها تفرض وقوع جريمة أصلية سابقة عليها حقق مرتكبها فائدة أو منفعة معينة، وهي مصدر الأموال غير المشروعة.

¹ فريد علواش، جريمة غسيل الأموال دراسة مقارنة، أطروحة الدكتوراه العلوم في الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2008-2009، ص ص 42-43.

² أحمد إبراهيم دهبان، يحي إبراهيم دهبان، موسوعة الجرائم الاقتصادية أساليب غسل الأموال التقليدية والحديثة مراحل وآليات الجريمة، الشروط الأساسية للجريمة، أركان الجريمة، ج2، د ط، الدهشان للمحاماة والاستشارات القانوني، 2025، ص 47.

ثانيا: جريمة غسل الأموال جريمة اقتصادية

الجريمة الاقتصادية هي كل فعل أو امتناع له مظهر خارجي يخل بالنظام الاقتصادي والائتماني للدولة يحظره القانون، فهي ترتبط بعلاقة طردية بعمليات التحرير الاقتصادي والمالي

ثالثا: جريمة تبييض الأموال جريمة منظمة وعابرة للحدود

باعتبار جريمة غسل الأموال من الجرائم الدولية الخطيرة والتي تعود سلبا على الاقتصاد الدولي نجد أنها في أغلب الحالات تكون جريمة منظمة تفرض تعدد الجناة ووحدة الجريمة ماديا ومعنويا بحيث يساهم كل واحد منهم بعنصر أو أكثر من العناصر المؤثرة في الجريمة، فهي تتم من خلال خبراء متخصصين على علم تام بقواعد الرقابة والإشراف في الدولة وما يوجد بها من ثغرات يمكن النفاذ بها، وعلى علم بفرض ومجالات الاستثمار والتوظيف والأصول التي توفر الأمان لهذه الأموال، كما تتسم بسرعة الانتشار الجغرافي، كما أنها تتواكب مع الثورة التكنولوجية، حيث تشهد تلك العمليات تطورا كبيرا في تكتيكها، وكذا بالتطور في وسائل التكنولوجيا التي تستخدم في نقل الأموال وتحويلها عبر الحدود.

رابعا: عمليات غسيل الأموال عملية مصرفية

لما للمصاريف من دور استراتيجي في هذه العمليات، حيث تتكاثر عمليات غسيل الأموال في المؤسسات المالية والمصرفية لما لها من جو الكتمان والسرية المفروضة عليها بينها وبين متعاملاتها، فظاهرة غسيل الأموال تعود بالفائدة على الدولة المستقبلة للأموال المهربة قصد تبييضها وتقنينها وإعادة صفها من جديد في الاقتصاد الوطني يمكن اعتبار المصرف مجرد مستودع للأموال القذرة، بل قد يصل الأمر إلى قيام المصرف باستثمار هذه الأموال في شتى المجالات وتمويل العديد من الأنشطة كما تساعد على زيادة معدل الجريمة المنظمة محليا ودوليا¹.

وهذا ما يجعلها معقدة ومتشابكة وذات بعد دولي، ويستخدم فيها وسائل فنية قابلة للتطور وغالبا ما تتم هذه العملية في إقليم دول مختلفة.

¹ فريد ناشف، جريمة تبييض الأموال من منظور التشريع الجزائري، مجلة الحقوق والحريات، جامعة البليدة 02، المجلد 10، العدد 1

2022، الجزائر، ص ص 768. 770.

المبحث الثاني

الوسائل التقنية المستحدثة في عملية تبييض الأموال

تعد الوسائل التقنية المستحدثة من أبرز العوامل التي ساهمت في تطور أساليب تبييض الأموال في البيئة الرقمية، حيث أتاح التقدم التكنولوجي للمجرمين استخدام أدوات حديثة لإخفاء مصادر الأموال غير المشروعة وتسهيل تداولها، كما أن انتشار المعاملات الإلكترونية زاد من صعوبة كشف وتتبع هذه الممارسات.

سنتطرق في هذا المبحث إلى العملات المشفرة كألية لتبييض الأموال (المطلب الأول) واستغلال المنصات والوسائل الرقمية في تبييض الأموال (المطلب الثاني)

المطلب الأول

العملات المشفرة كألية لتبييض الأموال

نظرا للجدل المتزايد حول العملات المشفرة خاصة البيتكوين ما تثيره من إشكالات قانونية واقتصادية سيتم في هذا المطلب تناول مفهوم العملات المشفرة وأنواعها وخصائصها، مع إبراز أهم الآليات التي يتم من خلالها استغلالها في عمليات التمويه ولهذا سنعالج في هذا المطلب مفهوم العملة المشفرة وأنواعها في (الفرع الأول) وخصائص العملات المشفرة في (الفرع الثاني) وآليات استخدامها في التمويه (الفرع الثالث)

الفرع الأول

مفهوم العملة المشفرة وأنواعها

للوصول إلى مفهوم العملة المشفرة والوصول إلى خصائصها واكتساب نظرة عامة عنها وجب البحث في معنى هذه العملات خاصة القانوني منه، لتمكين القارئ من معرفة معناها وتمييزها عن المصطلحات الأخرى سنعالج (أولا) تعريف العملات المشفرة وأنواع العملات المشفرة (ثانيا).

أولا: تعريف العملات المشفرة

لم يستقر الفقهاء والباحثين على مصطلح وتعريف موحدين لهذا النوع الجديد من العملات فقد أثار جدلا واختلافا من خلاف التعريف والمصطلح المناسبين¹، فهناك عدة تسميات لها فالمشاركة يصطلحون

¹ خالد بغداد، التنظيم القانوني للعملات المشفرة، (مذكرة ماستر) كلية الحقوق، المركز الجامعي مغنية، 2019، ص6

الفصل الأول: الإطار المفاهيمي والتقني لجريمة تبييض الأموال في البيئة الرقمية

عليها بالعملة المعماة أما في الغرب اصطلاحوا عليها تسمية العملات المشفرة ووصفها البعض الآخر بالأسول الرقمية ،واتجه فريق آخر لتسميتها بعملة الظل- لأنها لا يمكن لمسها ماديا ،أيضا هناك من يسميها بالعملات الرقمية أو الجديدة والمستحدثة والظاهرية وغيرها من التسميات ،أما المصطلحات الشائعة الاستخدام والمعروفة في الدراسات والمعاملات في الفضاء السيبراني هي العملات المشفرة أو الرقمية ¹.

كما أنه يقع خلط بين مفهوم العملات المشفرة Crypto Currencncies مع كل من العملات الرقمية Digital Currencncies والعملات الافتراضية Vurital Currencncies لكن هناك تباين واضح بين تلك الأنماط من العملات يوضح على النحو التالي:

1-العملات الرقمية Digital Currencncies : هي عملات ذات طابع إلكتروني وقيمة إلكترونية، يتم تداولها عبر الوسائط الرقمية مع إمكانية خضوعها لإطار قانوني ينظم إصدارها وتداولها.

2-العملات الافتراضية Vurital Currencncies : هي نوع من العملات الرقمية، يتم استخدامها داخل بيئات افتراضية محددة، لا تستند إلى أي غطاء قانوني كما لا تخضع لرقابة رسمية من جهة مختصة.²

3-العملات المشفرة Crypto Currencncies :بشكل عام لا يوجد تعريف موحد للعملة المشفرة وذلك راجع إلى الغموض المتعلق بالمفاهيم والمصطلحات المستحدثة حول هذا النوع من النقود لذا:

عرفها المشرع الجزائري ب" الأصول الافتراضية " واعتبرها قيما رقمية يمكن تداولها رقميا أو تحويلها ويمكن ان تستخدم لأغراض الدفع أو الاستثمار، كما أنه "لا تتضمن الأصول الافتراضية عمليات القيم الرقمية للعملات الورقية والأوراق المالية، وغيرها من الأصول المالية"³ وهذا ما جاء به المشرع الجزائري في تعديله الأخير ضمن القانون رقم 10-25 المؤرخ في 24 يوليو 2025 يعدل ويتم القانون 01-05 المؤرخ في 6 فيفري 2005.

¹ خالد بغداد، مرجع سابق، ص6.

² وديع أسامة وجدي، خصائص العملات المشفرة بين المنافع والتهديدات التنظيمية، المجلة العلمية للاقتصاد والتجارة، جامعة عين شمس مصر، العدد4، نوفمبر 2019، ص254.

³ القانون رقم 10-25، المؤرخ في 24 يوليو 2025، المعدل والمتمم للقانون رقم 01-05 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتها، ج ر، العدد 48، 2025.

الفصل الأول: الإطار المفاهيمي والتقني لجريمة تبييض الأموال في البيئة الرقمية

أ- عرفها بنك التسويات الدولية (BIS) بأنها عملات رقمية تتسم بالخصائص التالية:

-تعد من الأصول التي تحدد قيمتها وفقا لقوى العرض والطلب، وتشبه في مفهومها السلع كالذهب، إلا أن قيمتها الحقيقية قد تكون معدومة كما أنها لا تفرض أي التزام على الأفراد أو المؤسسات، ولا تحظى بدعم من أي جهة تنظيمية.

-يتم تداولها إلكترونيا بين الأفراد دون الحاجة إلى وجود وسطاء، كما أنها لا تخضع لإدارة أي جهة أو إشراف شخص معين.

ب-عرفتها مجموعة العمل المالي (FATF) بأنها: تمثيل رقمي للقيمة يمكن تداوله إلكترونيا، يستخدم كوسيلة للتبادل، ووحدة حساب، ومخزن للقيمة، إلا أنه لا يستند إلى أساس قانوني، ولا تضمنه أي دولة ويؤدي الوظائف المذكورة داخل مجتمع افتراضي لمستخدميه، ويختلف عن العملات القانونية في كونه لا يتمتع بغطاء قانوني.

ج-عرفها صندوق النقد الدولي بأنها: قيمة نقدية تخزن إلكترونيا سواءا في شكل وحدات ائتمانية أو في ذاكرة إلكترونية لصالح المستهلك، وبالتالي تعد العملة الرقمية شكلا جديدا من النقود، أي أنها البديل الإلكتروني للنقود الورقية والمعدنية ذات الطبيعة المادية.

د-عرفها البنك المركزي الأوروبي (ECB): بأنها تمثيل رقمي لقيمة معينة، لا تصدر عن البنوك المركزية أو مؤسسات الإقراض أو مصدري النقود الإلكترونية، ويمكن استخدامها في بعض الحالات كبديل للنقود وعليه يمكن القول إن العملة المشفرة تمثل قيمة نقدية تنشأ وتتداول إلكترونيا، ويتم تخزينها في وسائط إلكترونية، ولا تصدر عن البنك المركزي، وتعد بديلا للنقود الورقية والمعدنية.¹

ثانيا: أنواع العملات المشفرة

شهدت العملات المشفرة انتشارا واسعا، حيث ظهرت منها العشرات، غير أننا سنقتصر على عرض أبرزها:

¹أفتيحة بنابي، العملات المشفرة كوجه حديث للعملات الرقمية، تطبيقاتها وأثارها على المعاملات البنكية-بنك سيليكون فاليس نموذجاً-، مجلة اقتصاديات الأعمال والتجارة، جامعة محمد بوضياف المسيلة، العدد 1، مارس 2024، ص 49.

الفصل الأول: الإطار المفاهيمي والتقني لجريمة تبييض الأموال في البيئة الرقمية

1-البيتكوين: تعد عملة إلكترونية مشفرة، تشبه في استخدامها العملات التقليدية كالبيورو والدولار، إلى أنها تتداول حصريا عبر شبكة الأنترنت دون أن يكون لها وجود مادي.

2-البيروكوين: صممت لتقليل نسبة التضخم لتكون في حدود 1 بالمائة، وتعد أكثر استدامة مقارنة بباقي العملات الرقمية، وقد ظهرت سنة 2012، ويكمن اختلافها عن العملات الأخرى في أساليب الأمان وطرق معالجة البيانات.

3-الكوارك: تتميز بانخفاض قيمتها مقارنة بباقي العملات، حيث لا تتجاوز 0.05 دولار، ورغم ذلك تعد من أكثر العملات اعتمادا على التشفير، إذ تستخدم تسع جولات من التشفير لتعزيز الأمان والحفاظ على سرية الهوية، وقد ظهرت سنة 2013.

4-الماستر كوين: ظهرت سنة 2013، وجاءت نتيجة لبعض المشكلات الأمنية وعدم استقرار سعر البيتكوين.

5-الريبيل: تختلف عن باقي العملات، إذ لا يمكن تعدينها، وتستخدم كنظام دفع وشبكة لتحويل الأموال، وقد ظهرت سنة 2013.

6-أورورا كوين: تم إطلاقها سنة 2014 من طرف رجل أعمال أيسلندي، حيث قامت فكرتها على توزيع العملة على المواطنين، وقد بلغ سعر الواحدة منها 22.3 دولار، فيحين قدرت قيمتها السوقية ب حوالي 236.6 مليون دولار.¹

الفرع الثاني

خصائص العملات المشفرة

تتسم العملات المشفرة بمجموعة من الخصائص وهذا ما سنتناوله في هذا الفرع اللامركزية(أولا) والأمان والتشفير(ثانيا) الشفافية (ثالثا) السرعة والسهولة في التحويل وانخفاض التكاليف(رابعا) الخصوصية النسبية(خامسا) القلب العالي (سادسا) الحدود العالمية (سابعا).

تتمثل أهم الخصائص التي تميز العملات المشفرة فيما يلي²:

¹ عز الدين بوبكر مصطفى شرون، العملات المشفرة مستقبل المعاملات المالية -البيتكوين نموذجا-، مجلة المنهل الإقتصادي،

جامعة الوادي، العدد4، ديسمبر 2019، ص38.

² فتية بناي، مرجع سابق، ص ص 49-50.

أولاً: اللامركزية

أي أنها عملة رقمية وهمية لا تتمتع بوجود مادي ملموس، ولا تستند إلى قيمة ذاتية، ويتم إصدارها غالباً من قبل مؤسسات أو شركات خاصة، دون أن تكون مدعومة من طرف البنوك المركزية أو أي جهة حكومية، أي أنها لا تخضع لسلطة مركزية واحدة مثل البنوك، بل تعتمد على شبكة الحواسيب لتسيير المعاملات والتحقق منها.

ثانياً: الأمان والتشفير

أي أنها تمثل قيمة نقدية مخزنة إلكترونياً، حيث يتم إنشاؤها وتداولها عبر بيانات مشفرة لحماية المعاملات والبيانات حيث يتم تسجيل مختلف العمليات المالية ضمن سجل موزع على عدد كبير من الحواسيب، مما يجعل اختراقها أمراً بالغ الصعوبة مما يقلل احتمالات التزوير أو التلاعب بها.

ثالثاً: الشفافية

توفر العملات المشفرة درجة عالية من الأمان والشفافية، أي أن كل المعاملات مسجلة علناً، ويمكن لأي شخص التحقق منها، فيمكن رؤية حركة الأموال وتتبع التحويلات وغالباً ما تبقى هوية المستخدم غير ظاهرة مباشرة.

رابعاً: السرعة والسهولة في التحويل وانخفاض التكاليف

تمتاز العملات المشفرة بالسرعة في التحويل الأموال واستقبالها خاصة عبر الحدود الدولية كما ان تحويل يتم دون اللجوء إلى إجراءات معقدة كما هو الحال في الأنظمة التقليدية، كما يمكن مقارنتها بالعملات التقليدية كاليورو والدولار، من حيث إمكانية استخدامها في عمليات الشراء، إضافة إلى قابليتها للتحويل إلى عملات أخرى من خلال منصات التداول عبر الأنترنت، إلى جانب انخفاض تكاليف المعاملات فهي تكون برسوم أقل مما هي مفروضة في البنوك أو شركات التحويل.

خامساً: الخصوصية النسبية

توفر العملات المشفرة درجة من الخصوصية للمستخدمين، حيث يتم استخدامها من طرف الأفراد والشركات عبر شبكة الأنترنت فقط، كما تتيح لمستخدميها قدر من الخصوصية من خلال عدم الإفصاح عن هوياتهم، رغم أن ذلك لا يعني غياب التتبع بشكل تام.

سادسا: التقلب العالي

لا تخضع العملات المشفرة لرقابة أو إشراف سلطة مركزية عند إصدارها، وهو ما يجعل قيمتها قابلة للتقلب أي ان أسعارها تتغير بسرعة كبيرة خلال فترات زمنية قصيرة، بعكس العملات التقليدية مثل الدولار التي تكون أسعارها مستقرة.

سابعا: الحدود العالمية

فهي تتميز بطابعها العالمي (عابرة للحدود)، إذ لا ترتبط بإقليم جغرافي معين، ويمكن استخدامها في مختلف انحاء العالم.¹

هذه هي جل الخصائص والسمات التي تتسم وتمتاز بها العملات المشفرة.

الفرع الثالث

أليات استخدامها في التمويه

تعد العملات المشفرة إحدى أبرز ثمرات التطور التكنولوجي في العصر الرقمي، حيث تعتمد على تقنيات تشفير متقدمة وسجلات موزعة لتأمين المعاملات بشكل لا مركزي بعيدا عن سلطة البنوك المركزية هذا الطابع اللامركزي والمجهول في التعاملات الذي يمنح المستخدمين حرية وسرعة منخفضة التكلفة جعلها في الوقت نفسه أداة مزدوجة الاستخدام، إذ يتم استغلالها كآليات متطورة في التمويه والأنشطة غير المشروعة.

سنعالج في هذا الفرع خلاطات العملات المشفرة وكيفية عملها (أولا) وتبديل السلاسل (ثانيا) والتمويل اللامركزي (ثالثا)

أولا: خلاطات العملات المشفرة وكيفية عملها

تُستعمل خلاطات العملات المشفرة من قبل الأفراد والشركات بهدف إخفاء مصدر ووجهة العملات الرقمية الخاصة بهم، حيث توفر هذه الخدمات مستوى أعلى من الخصوصية مقارنةً بالمعاملات التقليدية على البلوكتشين، والتي تقوم أساساً على مبدأ الشفافية.

¹ فتيحة بنايبي، مرجع سابق، ص ص 49-50.

الفصل الأول: الإطار المفاهيمي والتقني لجريمة تبييض الأموال في البيئة الرقمية

وفي وقت قريب، كانت شركات العملات المشفرة تعمل دون التقيد باللوائح التقليدية للخدمات المالية، ومن بينها مبدأ "اعرف عميلك" (KYC)، وهو ما جعل المستخدمين الذين يتعاملون مع منصات لا تطبق هذه الإجراءات عرضة لمخاطر كبيرة.

وتقوم خلاطات العملات على فكرة إخفاء الهوية داخل نظام البلوكشين، إذ تتيح للمستخدمين إمكانية تبديل العملات و"تنظيفها" دون ترك آثار واضحة على السلسلة، ودون وجود سجل دقيق للمعاملات.

ونظرًا للطبيعة الخاصة لهذه الخدمات، فقد أصبحت محل استغلال من قبل المجرمين باعتبارها وسيلة حديثة وأمنة لتحويل العائدات غير المشروعة إلى عملات تبدو جديدة، ورغم أنها لم تُنشأ أساسًا لأغراض غير قانونية، إلا أنها أصبحت تُستخدم في الغالب لهذا الغرض.

وقبل التطرق إلى كيفية عمل هذه الخلاطات، يجدر التذكير بمراحل تبييض الأموال، باعتبار أن هذه الآليات تعكس بشكل كبير ما يحدث في تبييض الأموال التقليدي مرحلة الإيداع والتمويه والإدماج، مع اختلاف أن العمليات تتم في بيئة رقمية قائمة على البلوكشي، حيث تتم عملية تبييض الأموال عبر العملات المشفرة من خلال خطوات مشابهة، حيث يقوم المستخدمون بإيداع عملاتهم داخل الخلاط إلى جانب عدد كبير من العملات الأخرى، فيما يشبه عملية خلط جماعي للأموال. بعد ذلك، يعتمد الخلاط على تقنيات خوارزمية لإخفاء ملكية العملات ومصدرها والجهة التي ستقوم بسحبها.

وفي المرحلة الأخيرة، يتم إعادة توزيع العملات على المشاركين بشكل عشوائي، بحيث تبدو هذه العملات مشروعة وغير مرتبطة بأي سجلات مشبوهة، كما تتقاضى منصات الخلط رسومًا بسيطة مقابل هذه الخدمات، تتراوح عادة بين 1% و3% من قيمة المعاملات، مما يضمن استمرارية عملها¹.

ثانياً: تبديل السلاسل

مع التطور الكبير الذي يشهده مجال العملات المشفرة في السنوات الأخيرة، خاصة مع انتشار العديد من سلاسل الكتل وتعدد الأصول الرقمية، أصبح ما يعرف بتقنية "تبديل السلاسل" (Chain Hopping) من بين الطرق الأكثر تعقيداً لتبييض الأموال عن طريق العملات المشفرة.

وتقوم هذه التقنية أساسًا على تحويل الأموال بشكل متكرر بين عدة عملات رقمية أو عبر سلاسل كتل مختلفة، وذلك بهدف إخفاء مصدرها الحقيقي وجعل عملية تتبعها أكثر صعوبة بالنسبة للمحققين، وغالبًا ما

¹ Blog article: Crypto Mixer Money Laundering Is the Risk Worth the Reward?, IDnow Houton Jody

، <https://www.idnow.io/blog/crypto-mixer-money-laundering-risk-reward/>، Accessed March 27, 2026، time 23:30

الفصل الأول: الإطار المفاهيمي والتقني لجريمة تبييض الأموال في البيئة الرقمية

تتم هذه العمليات بسرعة كبيرة، مما يزيد من تعقيد تتبع مسار الأموال بشكل يدوي، ولتسهيل هذه العمليات، يعتمد المجرمون على مجموعة من الوسائل التقنية، من أهمها المنصات اللامركزية (DEX) التي تسمح بتبادل العملات بشكل مباشر دون الحاجة إلى وسيط، ودون فرض إجراءات التحقق من الهوية، وهو ما يساعد على تحويل الأموال غير المشروعة إلى أصول أخرى بسهولة وفي وقت قصير.

كما يتم الاعتماد على ما يعرف بالجسور بين السلاسل، والتي تسمح بنقل الأصول الرقمية من شبكة إلى أخرى، من خلال تجميد الأصل في شبكة معينة وإصدار ما يقابله في شبكة أخرى، وهو ما يزيد من صعوبة تتبع هذه الأموال قانونياً، إلى جانب ذلك توجد خدمات تبديل العملات التي تتيح تحويل الأصول بين مختلف الشبكات دون الخضوع لرقابة صارمة أو إجراءات تحقق، وهو ما جعلها خياراً مفضلاً لدى بعض المجرمين مقارنة بوسائل أخرى مثل خلاطات العملات.

ورغم أن تقنية تبديل السلاسل في حد ذاتها لا تعتبر نشاطاً غير قانوني، بل تُستعمل بشكل عادي داخل نظام العملات المشفرة، إلا أن بعض الجهات تستغلها لإخفاء أموال ناتجة عن أنشطة غير مشروعة، مثل تبييض الأموال والاحتيال أو الاختراق أو غيرها من الجرائم، كما أن بعض العمليات لا تعتمد على وسيلة واحدة فقط، بل يتم الجمع بين عدة تقنيات في نفس الوقت، مثل استعمال المنصات اللامركزية ثم نقل الأموال عبر الجسور، ثم تحويلها مرة أخرى، وهو ما يزيد من تعقيد عملية التتبع.

وبالتالي، يمكن القول إن تبديل السلاسل يُعد من الوسائل الفعالة في تبييض الأموال الرقمية، خاصة في ظل صعوبة تتبع هذه العمليات وغياب وسائل تقنية متطورة لدى بعض الجهات المختصة¹

ثالثاً: التمويل اللامركزي (DeFi)

مع تطور المجال المالي، ظهرت بعض الانتقادات الموجهة للنظام التقليدي، وهو ما أدى إلى البحث عن بدائل حديثة، كان من بينها التمويل اللامركزي (DeFi)، الذي أصبح من أبرز مكونات نظام العملات المشفرة.

ويقصد به نظام مالي يقوم على التعامل المباشر بين المستخدمين دون الحاجة إلى وسيط، ويعتمد على تقنية البلوكشين والعقود الذكية التي تسمح بتنفيذ المعاملات بشكل تلقائي، كما يوفر هذا النظام خدمات مشابهة للتمويل التقليدي، مثل الإقراض والاقتراض والتداول والتأمينات.

¹Blog article Chain-Hopping : The Defining Money Laundering Method of Modern Crypto Crime «Elliptic» ، <https://www.elliptic.com/> ، Accessed March 30, 2026، time 22:04

الفصل الأول: الإطار المفاهيمي والتقني لجريمة تبييض الأموال في البيئة الرقمية

ويتميز التمويل اللامركزي بعدة خصائص تجعله مختلفاً عن النظام التقليدي، من بينها عدم الاعتماد على مؤسسات وسيطة، وإمكانية الوصول إليه بسهولة دون إجراءات معقدة، إضافة إلى الشفافية في المعاملات، حيث يتم تسجيلها على شبكات عامة. كما يمنح المستخدمين تحكماً مباشراً في أموالهم، ويتميز بسرعة العمليات وانخفاض تكلفتها.

ويعتمد DeFi في عمله على مجموعة من الأدوات، من أهمها العقود الذكية التي تنفذ العمليات تلقائياً والتطبيقات اللامركزية التي تتيح استخدام هذه الخدمات، إلى جانب مجتمعات السيولة وصناع السوق الآليين الذين يسهلون عمليات التداول داخل هذا النظام.

ورغم هذه المزايا المتعددة لهذا النظام، إلا أن هذا النظام يُستغل في أنشطة غير مشروعة، مثل تبييض الأموال للتهرب من المتابعة القانونية، خاصة بسبب غياب الرقابة المركزية وصعوبة تتبع العمليات¹.

المطلب الثاني

استغلال المنصات والوسائل الرقمية في تبييض الأموال

أدى التطور السريع في المجال الرقمي إلى ظهور وسائل حديثة متعددة في المعاملات المالية حيث لم تعد تقتصر على الأساليب التقليدية بل امتدت لتشمل فضاءات رقمية متنوعة، سنتناول في هذا المطلب دراسة أهم صور استغلال الوسائل الرقمي في تبييض الأموال من خلال التجارة الإلكترونية والألعاب الرقمية، وبنوك الأنترنت ووسائل التحويل الإلكتروني، إضافة إلى بطاقات الدفع الذكية.

لذا سنتناول في هذا المطلب فرعين، فجاء (الفرع الأول) بعنوان: استغلال التجارة الإلكترونية في عملية تبييض الأموال، أما (الفرع الثاني) فقد عنون بتبييض الأموال عن طريق الألعاب الرقمية، أما (الفرع الثالث) فجاء بعنوان استخدام البنوك والانترنت في عمليات تبييض الأموال واستخدام التحويل الإلكتروني للأموال في عمليات تبييض الأموال في (الفرع الرابع) واستخدام بطاقات الدفع الذكية في عمليات تبييض الأموال في (الفرع الخامس).

¹ Blog article What Is DeFi in Crypto ،Cryptopolitan Nelluis irene ،august 2025

<https://www.cryptopolitan.com/ar/what-is-defi-in-crypto/?> Accessed March 30, 2026·time 23:30

الفرع الأول

استغلال التجارة الإلكترونية في عملية تبييض الأموال

تعد التجارة الإلكترونية وسيلة حديثة استغلها مرتكبو الجرائم لتنفيذ عمليات تبييض الأموال مستفيدين من السرعة الفائقة في تنفيذ المعاملات وصعوبة تعقب هوية الأطراف المشاركة عبر الانترنت ولمعرفة هذا سنتطرق إلى تعريف التجارة الإلكترونية (أولا) استغلال التجارة الإلكترونية في عملية تبييض الأموال (ثانيا).

أولا. تعريف التجارة الإلكترونية

يمكن تعريف التجارة الإلكترونية بأنها كل معاملة تجارية بين البائع والمشتري ساهمت فيها شبكة الإنترنت جزئيا أو إجماليا كالتزود بمعلومات عن طريق شبكة الإنترنت أو شبكات تجارية أخرى بشأن خدمة أو سلعة معينة لاقتنائها لاحقا، سواء تم التسديد إلكترونيا أو نقدا عند التسليم أو بطريقة أخرى وهنا يجب عدم الخلط بين التجارة الإلكترونية E-commerce والقيام بإنجاز الأعمال إلكترونيا E-business التي تعني القيام بمهام تنفيذ الأعمال على الشبكة باستخدام تكنولوجيات الإنترنت بهدف الربح¹.

وقد عرفت منظمة التجارة العالمية WTO بأنها عملية إنتاج وتوزيع وبيع وتداول المنتجات من خلال شبكة اتصال، وقد شمل هذا التعريف جميع الأنشطة التجارية من توريد أو بيع أو تبادل أو تداول وبيع السلع عن طريق شبكات الاتصال كالإنترنت.

كما عرفت منظمة التعاون الاقتصادي OECD في التقرير الصادر سنة 1998 بأنها كل الأنشطة التجارية التي تشمل الصفقات التجارية، اتفاقات التمويل والمفاوضات الجارية والعقود التجارية المبرمة بين الأشخاص أو الإدارات عن طريق المعالجة الإلكترونية للبيانات المقروءة أو الصوتية شاملة المنتجات والسلع والخدمات.

¹ إبراهيم بختي، التجارة الإلكترونية: مفاهيم وإستراتيجيات التطبيق في المؤسسة، ط1، ديوان المطبوعات الجامعية، الجزائر 2005، ص42.

الفصل الأول: الإطار المفاهيمي والتقني لجريمة تبييض الأموال في البيئة الرقمية

وعرفها الاتحاد الأوروبي EU بأنها كل الأنشطة التي تتم بواسطة وسائل إلكترونية التي تتم بين المشروعات التجارية والمستهلكين أو بين الإدارات الحكومية.¹

ولقد ورد للتجارة الإلكترونية تعريفا آخر في التشريع الجزائري في المادة 6 من القانون رقم 18-05 بأنها: "النشاط الذي يقوم بموجبه مورد إلكتروني باقتراح أو ضمان توفير السلع والخدمات عن بعد لمستهلك إلكتروني عن طريق الاتصالات الإلكترونية"²

ومن خلال هذا التعريف، يظهر أن المشرع الجزائري ركز على المورد الإلكتروني باعتباره الفاعل الرئيسي في هذا النوع من التجارة، وهو ما يجعله يختلف عن التاجر التقليدي المنظم في القانون التجارة غير أن هذا الأخير لا يستبعد تماما، إذ يمكنه استخدام وسائل الاتصال الإلكترونية في الترويج لمنتجاته أو إبرام بعض معاملاته، دون أن يعد بالضرورة ممارسا للتجارة الإلكترونية بالمفهوم القانوني الدقيق.³

ثانيا: استغلال التجارة الإلكترونية في عملية تبييض الأموال

ترتبط التجارة الإلكترونية بعلاقة وثيقة بجرائم تبييض الأموال، وذلك بالنظر إلى طبيعة المعاملات التي تتم في إطارها، والتي تعتمد أساسا على استخدام النقود الإلكترونية ووسائل الدفع الحديثة، فهذه الوسائل تساهم في تسهيل وتسريع عمليات تسوية المدفوعات، كما تقلل من الحاجة إلى التعامل بالنقود التقليدية، وهو ما يؤدي بدوره إلى توسيع نطاق التبادل التجاري عبر شبكة الإنترنت.

ومن جهة أخرى، تتيح التجارة الإلكترونية إمكانية تحويل مبالغ مالية كبيرة بين حسابات مختلفة بكل سهولة وفي وقت وجيز، خاصة في ظل غياب الاتصال المباشر بين أطراف المعاملة، وهذا ما يجعلها بيئة ملائمة يمكن استغلالها من قبل مرتكبي جرائم تبييض الأموال، من خلال الاعتماد على وسائل دفع إلكترونية

¹ التجارة الإلكترونية، الموسوعة السياسية، 2021، -/https://political encyclopedia.org/dictionary/ : التجارة الإلكترونية، أطلع عليه بتاريخ 2026/04/04، على الساعة 15:07 .

² القانون رقم 18-05، المادة 6، المؤرخ في 10 ماي 2018، المتعلق بالتجارة الإلكترونية، ج ر، العدد 28، 2018.

³ أيمن بوزانة، وفاء حمدوش، التجارة الإلكترونية في سياق القانون رقم 18-05 والمراسيم التنفيذية المتعلقة بالسجل التجاري الإلكتروني في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة عنابة، العدد 1، جوان 2021، ص 1837.

توفر قدرا من السرية والأمان، بما يسمح بإخفاء المصدر غير المشروع للأموال وإدماجها في الدورة الاقتصادية بشكل يصعب تتبعه من قبل الجهات الرقابية¹.

الفرع الثاني

تبييض الأموال عن طريق الألعاب الرقمية

تعد العناصر والقطع الفنية داخل الألعاب والعملات الافتراضية المستخدمة فيها غالبًا ذات قيمة حقيقية، إذ يمكن استغلالها لتحريك الأموال أو استثمار عوائد غير مشروعة ومع ذلك، لا توجد توجبهات واضحة لما يجب على مشغلي الألعاب فعله لكشف النشاط الإجرامي أو منعه، مما يخلق فرصة لاستغلال هذه الألعاب في عمليات تبييض الأموال، وخاصة الألعاب متعددة اللاعبين عبر الإنترنت التي تعتمد على تقمص الأدوار، في عمليات غسل الأموال كلعبة: Clash of Clans، freefire، pubg mobile، Second Life، Clash Royale Fortnite.... إلخ.

بحسب المحلل المختص بالجرائم الإلكترونية جان-لوب ريشيه، فقد أظهرت التحقيقات في منتديات القراصنة أنه من خلال أنظمة العملات الافتراضية داخل الألعاب عبر الإنترنت، يمكن للمجرمين تحويل أموال افتراضية بين دول مختلفة، ما يسمح بتسريب الأموال غير المشروعة بطريقة تشبه انتقال المال "القذر" إلى أماكن أقل رقابة، كما يحدث عند الضغط على بالون مضغوط وانتقال الهواء إلى مكان آخر.

وتكمن قدرة الألعاب عبر الإنترنت على تسهيل غسل الأموال في حقيقة أن بعض العناصر داخل اللعبة تحمل قيمة فعلية خارج نطاق اللعبة. فمثلاً، القطع الأثرية تمنح الشخصيات قدرات إضافية مثل السيوف والدروع وجرعات السحر، أو العملات الافتراضية التي يمكن شراؤها وبيعها مقابل عملة نقدية حقيقية كالريال أو الدولار. تُعرف هذه العمليات باسم «المعاملات الدقيقة»، وهي شائعة في الألعاب المجانية التي توفر عناصر مدفوعة داخل اللعبة.

علاوة على ذلك، يتجه عدد متزايد من الألعاب مثل: pubg mobile، Entropia Universe، و Second Life إلى نظام المشتريات داخل اللعبة على نمط مقامرة، حيث تُباع قطع محددة عشوائيًا، ولا

¹ كمال مهدي، دريس باخويا، دور الوسائط التكنولوجية في انتشار جرائم تبييض الأموال وأليات مكافحتها، المجلة الإفريقية للدراسات القانونية والسياسية، جامعة أدرار، العدد2، ديسمبر 2018، ص178.

يُعرف محتواها للمشتري إلا بعد الشراء، ما يفتح المجال أمام استخدام هذه المشتريات كوسيلة غير مباشرة لغسل الأموال¹.

الفرع الثالث

استخدام بنوك الأنترنت في عمليات تبييض الأموال

من أهم الوسائل الحديثة في تبييض الأموال في البيئة الرقمية ما يعرف ببنوك الأنترنت أو نظام (E.Banking) وهي وسائل تتيح إجراء العمليات المالية عبر شبكة الأنترنت دون الحاجة إلى وجود مقر مادي أو موظفين إذ تقوم بدور الوسيط في تنفيذ التحويلات المالية مما يسمح لمباضي الأموال بنقل وتحويل مبالغ مالية ضخمة بسرعة وأمان أكبر².

تتميز بنوك الأنترنت بإمكانية إجراء عمليات مصرفية وتحويل الأموال إلى مختلف أنحاء العالم دون التقيد بمكان أو زمان، وهو ما استغله مجرمو تبييض الأموال في البيئة الرقمية لإجراء تحويلات متعددة ومعقدة عبر عدة بنوك، مما يزيد من صعوبة تعقب المعاملات المالية والكشف عن حقيقتها.

الفرع الرابع

استخدام التحويل الإلكتروني للأموال في عمليات تبييض الأموال

يلجأ المجرمون لتبييض أموالهم إلى أسلوب التحويل الإلكتروني للأموال بسبب الثغرات التي تعتري هذا النظام، ومنها إيداع وتحويل الأموال لدى البنوك في بلد آخر من دون الإعلان عن هوياتهم.

ويتمثل السلوك الإجرامي في مثل هذه الحالة في أنه بعد قيام الجناة بإيداع أموالهم لدى البنوك بطريقة آمنة، يقومون بتحويلها برقيا إلى حسابات شركات وهمية في بلد آخر يضمن نظامه السرية التامة في المعاملات البنكية، ولا يسمح لأي جهة بالاطلاع على دفاترها أو هويات من تعاملها أو تتبع حركات حساباتها، وقد استغل المجرمون انشغال السلطات و الجهات المخولة بمكافحة عمليات تبييض الأموال بتتبع تبييض

¹ Blog article 'Cybercrime and Virtual Economies in Online Gaming London: Royal United Services Institute (RUSI) Anton Moiseienko and Kayla Izenman, October 11, 2019', https://static.rusi.org/20191011_newsbrief_vol39_no9_moiseienko_and_izenman_web.pdf?utm.com, Accessed March 30, 2026, time 23:30

² المختار بن قوية، جريمة تبييض الأموال بين الأساليب التقليدية والتكنولوجيات الحديثة، المجلة المتوسطة للقانون والاقتصاد، جامعة ألكلي محند أولحاج، البويرة، المجلد 9، العدد 1، 2024، ص 61.

الأموال باستخدام النقود الورقية لكي يقوموا بعمليات التبييض عن طريق التحويلات الإلكترونية خاصة وأن هذا النظام يضمن عدم التعرف على طبيعة المعاملات التي تتم ولا الغرض منها.¹

الفرع الخامس

استخدام بطاقات الدفع الذكية في عمليات تبييض الأموال

يعتبر الدفع عبر البطاقات الذكية من أحدث وسائل الدفع الإلكتروني، كما أن للبطاقات الذكية عدة نماذج منها البطاقات البنكية التقليدية ، ومنها ما هو مرتبط بالمحافظ الإلكترونية مثل البطاقات التي توفرها منصات pyypl،redotpay والتي تعد امتدادا حديثا للبطاقات الذكية، كما أن لهذه البطاقات العديد من الخصائص التي تميزها عن البطاقات الأخرى الأمر الذي يغري المجرمين لاستخدامها في عمليات تبييض الأموال، حيث أنها تشبه حافظة النقود الحقيقية التي تضم أموالا وأوراقا نقدية يحملها الشخص ، إلى أنها تحمل نقودا إلكترونية ، كما أنه يمكن لحاملها سحب اعتمادات مالية إلكترونية أو استخدامها في عمليات الشراء، وما يدفعه مستعمل البطاقة يخصم من النقود الموجودة قيمتها في البطاقة ، كما يمكن إعادة شحنها من أي منفذ إلكتروني (منصة بايننس على سبيل المثال)،ومما لاشك فيه أن هذه الوسيلة سهلة للقيام بعمليات تبييض الأموال إذ يمكن لحامل هذه البطاقات استهلاك قيمتها في مشتريات باهظة الثمن، ثم يقوم بإعادة شحنها بأموال مودعة لدى مصرفه الإلكتروني بواسطة المال الذي يرغب بتدويره وتبييضه.²

بالإضافة إلى هذه الأساليب المستحدثة توجد أساليب التقليدية والتي تتمثل في العديد من الطرق القديمة المكشوفة لأجهزة الرقابة والمساءلة، وتعتبر تقليدية في استخدامها من جهة، ومقارنة مع الأساليب الحديثة من جهة أخرى، نذكر منها³:

استغلال العلاقات الإنسانية والموضوعية (أولا) والأساليب التجارية (ثانيا)

¹ ذهبية لعجال، الأساليب الحديثة لتبييض الأموال في ظل التطور التكنولوجي، مجلة الاجتهاد القضائي، جامعة بسكرة، العدد 25 جانفي 2021، ص ص 905-908.

² المرجع نفسه، ص 911.

³ المختار بن قوية، مرجع سابق، ص 57.

أولاً: استغلال العلاقات الإنسانية والموضوعية

حيث يتم تواطؤ غاسلو الأموال مع موظفي وإدارات المصارف، فضلاً عن تهريب وتبادل العملات، واستغلال ذلك لتبديل الأموال غير المشروعة بأموال مشروعة، من خلال فتح حسابات متعددة باسمه أو باسم طرف ثالث، يتم استغلال حساباته لنفس الغرض، وتدخل هذه العلاقات في نظام المشاركة في تبييض الأموال.

1- استخدام الشركات الوهمية: وهي شركات مؤسسة بطريقة قانونية، غير أنها لا تمارس في الواقع أية نشاطات فعلية أو مشاريع، بحيث يتم فتح حسابات باسم الشركة داخلياً وخارجياً.

2- تهريب العملة: باستخدام كافة الطرق كتضخيم الفواتير، أو شراء مشروعات وهمية في الخارج، أو بإدخالها في السوق السوداء للعملة، أو عن طريق الحسابات البنكية المعتمدة والتي تسمح بتحويلها إلى الخارج.

3- الكازينوهات وأماكن لعب القمار: حيث تعد المقامرة طريقة فعالة في غسيل الأموال، وتتم عن طريق شراء رقائق الكازينو والاحتفاظ بها لمدة من الزمن ثم يعود ليقبض ثمنها بشيكات تحول إلى حسابه المصرفي، أو لحساب آخر.

ثانياً: الأساليب التجارية

ويتم دمج أو إعادة دمج الأموال المشبوهة باتباع الكثير من الطرق والأساليب التجارية نذكر منها¹:

1- الدين المضمون: وتقوم على وجود مؤسسات مالية مشبوهة تعتمد على إقراض أموال كثيرة بمعدلات فائدة منخفضة، مقابل أن يأخذ المقترض مبلغاً أكبر من المبلغ الذي يحتاجه، ثم يقوم باستخدام الفائض بشراء سندات خزانة أمريكية أو أوروبية لا توزع فوائد (سندات نمو) تصل عند نهاية مدتها إلى قيمة القرض، وفي النهاية تكون المؤسسة قد استطاعت ضخ كميات كبيرة من الأموال القذرة إلى نظام مصرفي شرعي

2- دفع الضرائب: يحصنها من شبهة الأموال القذرة ويمنع المؤسسات من الادعاء أنها تمثل إيرادات أنشطة إجرامية .

¹ المختار بن قوية، مرجع سابق، ص 57.

الفصل الأول: الإطار المفاهيمي والتقني لجريمة تبييض الأموال في البيئة الرقمية

3-بنوك الواجهة: وتقوم هذه الطريقة بامتلاك المجرم لبنك خاص، ويتم ضخ الأموال فيه، ثم يقوم البنك بإجراء مجموعة من العمليات على هذه الأموال حتى يتم تبييضها بشكل تام، ثم تتم بعد ذلك عمليات التحويل الإلكتروني لهذه الأموال.

4-ملكية الأدوات المالية: وتقوم على أساس مجموعة من شركات الوساطة تقوم بتجميع العملاء وبيع كميات كبيرة من الأسهم والسندات الوهمية تحت مسميات أوراق مالية ذات قيمة وهي في الواقع بلا قيمة وقد لا يمكن بيعها في أي مكان.

5-القرض العائد: وتقوم هذه الطريقة على وضع الأموال القذرة في مؤسسة مالية قانونية في الخارج، ثم يشتري مشروعاً في بلده، ويقترض من تلك المؤسسة المبلغ الضروري، ثم يقوم بتسديد القرض من الأموال القذرة التي أودعها على فترات، وبذلك يكون قد أدمج أمواله، وأدخلها إلى بلده بطريقة تبدو مشروعة ولا تثير أي شك.

6-الصفقات النقدية: ك شراء السيارات الفخمة الباهظة الثمن، أو القطع الفنية النادرة، أو تحويل العملة المحلية إلى ذهب أو مجوهرات، أو غير ذلك مما يسهل بيعه في الخارج ثم يتم إيداعها في البلد الأجنبي ذاته.

7-الفواتير المزورة: من خلال شراء أو بيع السلع والخدمات بين شركتين عن طريق عمليات صورية، حيث يقوم بمبيض الأموال بشراء سلع من الشركة التي يريد تحويل الأموال إليها، ويكون ذلك بعدة صور؛ كرفع قيمة السلع أو الخدمات الواردة في الفاتورة، ويكون الفرق هو المال المغسول؛ أو عن طريق فواتير مزورة كلياً يكون المبلغ في هذه الحالة هو المال المغسول¹، ومن خلال سبق ذكره حول الأساليب الحديثة والتقليدية في عملية تبييض الأموال نستنتج أن الفرق بينهما يكمن في الجدول التالي:

تبييض الأموال في البيئة الرقمية	تبييض الأموال التقليدي
يعتمد على الانترنت والعملات الرقمية	يعتمد على البنوك التقليدية والعقارات
يتم عن بعد إلكترونياً	يحتاج تنقلات ومعاملات مادية
أصعب بسبب إخفاء الهوية	أسهل نسبياً في التتبع
سريع جداً وعابر للحدود	أبطأ في التحويلات
صعوبة الرقابة على المنصات الرقمية	رقابة مصرفية مباشرة

¹ المختار بن قوية، مرجع سابق، ص 57

خلاصة الفصل الأول

تعد جريمة تبييض الأموال عملية معقدة تهدف إلى إضفاء طابع الشرعية على أموال مكتسبة من أنشطة غير مشروعة، وتتم عملية تبييض الأموال من خلال عمليات معقدة تتم عبر مراحل أساسية ثلاث ففي المرحلة الأولى وتسمى مرحلة الإيداع يتم فيها إدخال الأموال القذرة النقدية إلى النظام المالي المشروع (بنوك، شركات) أما في المرحلة الثانية يتم إخفاء مصدر الأموال وتسمى هذه المرحلة بالتمويه أما في المرحلة الأخيرة وتسمى بمرحلة الإدماج ويتم فيها إعادة استثمار الأموال المغسولة في الاقتصاد الرسمي (عقارات، شركات) لتظهر كأنها أموال طبيعية ومما تتسم به هذه الجريمة أن لها خصائص معقدة تجعل من مكافحتها تحديا كبيرا للسلطات والجهات الرقابية.

ولقد استغل المبيضون التطور التكنولوجي (التكنولوجية المالية) لتفادي الرقابة المصرفية التقليدية ومن أبرز الوسائل هي: العملات الرقمية والمشفرة التي تمثل قيمة نقدية تنشأ وتتداول إلكترونيا ويتم تخزينها في وسائط إلكترونية ولا تصدر عن البنك المركزي وتعد بديلا للنقود الورقية والمعدنية، فاستخدم البيوتكوين وغيرها لإجراء تحويلات دولية سريعة ومجهولة الهوية، إضافة إلى الاعتماد على خلطات العملات التي تخط الأموال المشبوهة مع أخرى نظيفة لإخفاء مسارها ومن الوسائل المستخدمة أيضا المصرفية عبر الأنترنت والتحويلات الإلكترونية، فتم إنشاء حسابات بنكية عبر الأنترنت بهويات مزورة أو مستعارة، إضافة إلى تفتيت المبالغ الكبيرة إلى مبالغ صغيرة وتحويلها إلكترونيا لتجنب لفت الانتباه، ومن الوسائل المستخدمة كذلك في عملية تبييض الأموال الوسائل التقنية المالية مثل أجهزة الصراف المالي فاستخدمت في الإيداع النقدي المتكرر، كما استخدمت البطاقات مسبقة الدفع محملة بمبالغ صغيرة لإجراء مشتريات دولية ومن الوسائل أيضا شراء أصول داخل الألعاب بعملات افتراضية تم إعادة بيعها مقابل عملات حقيقية وأخيرا استعمل التمويل الجماعي كآلية في تبييض الأموال لإنشاء حملات تبرع وهمية لدمج الأموال المشبوهة ضمن تبرعات.

فجريمة تبييض الأموال جريمة متجددة، حيث انتقل المبيضون من الطرق التقليدية إلى التقنيات الرقمية المتقدمة، هذا التطور يفرض ضرورة تحديث تشريعات مثل قانون الوقاية من تبييض الأموال الجزائري، واعتماد سياسات رقابية قائمة المخاطر وتكنولوجيات الذكاء الاصطناعي لرصد المعاملات المشبوهة بدقة وسرعة وهذا ما سنعالجه في الفصل الثاني لاحقا.

الفصل الثاني

آليات مكافحة جريمة تبييض الأموال
في البيئة الرقمية وإشكالات الملاحقة

الفصل الثاني

آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة

تعد جريمة تبييض الأموال عبر التكنولوجيات الحديثة طريقة عصرية للجرائم المستحدثة، وأخذت هذه الجريمة تزداد في ظل العولمة، حيث أصبحت تنقل الأموال عبر الحدود بسهولة وسرعة مما صعب مكافحتها، والسيطرة عليها، وقد أدى ذلك إلى السعي لوضع قوانين وإجراءات وطنية منها وأخرى دولية للمكافحة والحماية من هذه الجريمة.

وتجدر الإشارة إلى أن التحديات المتعلقة بمكافحة هذه الجريمة مستمرة ومتغيرة باستمرار، حيث تضطر الجهات المعنية إلى مواكبة التطورات التكنولوجية وتحديث آليات المكافحة لحماية الاقتصاد الوطني والدولي.

وهذا ما سنتطرق إليه في هذا المبحث من خلال معرفة الجهود الوطنية والدولية لمكافحة جريمة تبييض الأموال في البيئة الرقمية (المبحث الأول) وتحديات الإثبات والملاحقة في جريمة تبييض الأموال في البيئة الرقمية (المبحث الثاني).

المبحث الأول

الجهود الوطنية والدولية لمكافحة جريمة تبييض الأموال في البيئة الرقمية

تعد جريمة تبييض الأموال في البيئة الرقمية بأنها مرتبطة بتكنولوجيا المعلومات لارتكاب نشاط غير قانوني يصعب كشفها بسبب التطور التقني وتجاوزها للحدود الدولية، ولمواجهة هذا الخطر عملت الهيئات والدول على وضع قوانين وتشريعات تنظيمية وإجراءات وقائية تهدف إلى مكافحة جريمة تبييض الأموال في البيئة الرقمية وتوفير الحماية اللازمة من الناحية التقنية.

وهذا ما سنتطرق إليه من خلال الجهود الوطنية والتدابير الوقائية لمكافحة جريمة تبييض الأموال في البيئة الرقمية (المطلب الأول) الجهود الدولية لمكافحة جريمة تبييض الأموال في البيئة الرقمية (المطلب الثاني).

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

المطلب الأول

الجهود الوطنية والتدابير الوقائية لمكافحة الجريمة تبييض الأموال في البيئة الرقمية

في ظل التطور الرقمي المتسارع الذي تشهده الجزائر أصبحت جريمة تبييض الأموال من التهديدات الحديثة العابرة للحدود، لما لها من آثار على الأمن الوطني والاقتصادي مما دفع الدولة الجزائرية إلى تبني استراتيجية وطنية شاملة لمكافحتها، ولهذا سنتطرق في هذا المطلب الجهود الوطنية لمكافحة جريمة تبييض الأموال في البيئة الرقمية (الفرع الأول) والتدابير الوقائية (الفرع الثاني).

الفرع الأول

الجهود الوطنية لمكافحة جريمة تبييض الأموال في البيئة الرقمية

يقوم المشرع الجزائري في مجال مكافحة تبييض الأموال على تجريم الفعل نفسه، وفرض آليات وقائية ورقابية للحد منه، مع تعزيز صلاحيات التبليغ والتحري لذا سنتحدث في هذا الفرع عن المكافحة التشريعية للجريمة تبييض الأموال في البيئة الرقمية (أولا) والهيئات المكلفة لمكافحة جريمة تبييض الأموال في البيئة الرقمية (ثانيا).

أولا: المكافحة التشريعية للجريمة تبييض الأموال في البيئة الرقمية

سعت الجزائر إلى تعزيز مكافحة جريمة تبييض الأموال في البيئة الرقمية من خلال اعتماد آليات تتماشى مع التحول الرقمي والتحديات الأمنية الحديثة.

1- قانون العقوبات:

بدأ المشرع الجزائري في مواكبة التطورات التكنولوجية من خلال إدخاله مجموعة تعديلات على القانون العقوبات بإدراج قسم خاص يتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات¹ حيث تناول الجرائم التي يكون أساسها المعالجة الإلكترونية وحدد لها الجزاءات العقابية، فهو لم ينص صراحة على تبييض الأموال في البيئة الرقمية، لكن باعتبار أن الجريمة تحصل عن طريق الأنظمة المعلوماتية فهي إذن لها نفس العقوبات.

¹ مهدي رضا، الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري، مجلة ايليزا للبحوث والدراسات، جامعة زيان عاشور،

الجلفة، المجلد 6، العدد 2، 2021، ص 116.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

وبالرجوع لجريمة تبييض الأموال المنصوص عليها في قانون العقوبات، فنجد حدها من العقوبات تخص الشخص الطبيعي والشخص المعنوي فأورد عقوبات أصلية يمكن للقاضي النطق بها، وأخرى تكميلية للعقوبات الأصلية.

وبموجب القانون 01-09 المؤرخ في 25 فبراير 2009 المعدل والمتمم للأمر 66-156 المتضمن قانون العقوبات المادة 389 حيث نصت على العقوبة المسطرة على القائمين بهذه العملية مكرر 1 على ما يلي: "يعاقب بالحبس من 5 سنوات إلى 10 سنوات وغرامة من 1000000 إلى 3000000 دج"¹ أما المادة 389 مكرر 2 فأحكامها تعتبر مشددة بالنسبة لمرتكب جريمة تبييض الأموال باعتبار أن الجريمة التي قام بها إما هناك ظرف عود، استغلال منصب مهني في الجريمة، أو الجريمة كانت مرتكبة في إطار الجريمة المنظمة، وعليه قرر لها المشرع الحبس من 10 إلى 20 سنة وقام بزيادة القيمة النقدية المقدرة بـ: 4 إلى 8 ملايين دينار جزائري².

وفي المادة 389 مكرر 4 نص المشرع أنه على الجهات القضائية المختصة مصادرة الوسائل المستخدمة في عملية التبييض، وكذلك العائدات التي نتجت عن هذه الجريمة وهي من العقوبات التكميلية المقررة والمنصوص عليها بالإضافة إلى العقوبة الأصلية وحرص على أن يتم حجز الوسائل المستعملة حتى في حالة فرار المجرمين أو بقائهم مجهولين³.

ونصت المادة 389 مكرر 6 يعتبر الحكم بالمنع من الإقامة من العقوبات التكميلية بالنسبة للأشخاص الأجانب، سواء بصفة مؤقتة محددة بعشر سنوات، أو المنع بصفة دائمة وهذا تعتبر هذه العقوبات مسطرة على الأشخاص الطبيعيين، وكذلك يمكن تسليط أكثر من عقوبة تكميلية هذا بموجب المادة 389 مكرر 5 وكذلك العقوبات التكميلية المنصوص عليها في المادة 9 حيث يمكن القيام بـ⁴:

- الحجر القانوني.

¹ القانون رقم 01-09 المادة 389، المؤرخ في 25 فبراير 2009 المعدل والمتمم للأمر 66-156 المؤرخ 8 يونيو 1966، المتضمن قانون العقوبات ج ر، العدد 15، 2009.

² القانون رقم 01-09 المادة 389، المؤرخ في 25 فبراير 2009 المعدل والمتمم للأمر 66-156 المؤرخ 8 يونيو 1966، المتضمن قانون العقوبات ج ر، العدد 15، 2009.

³ القانون رقم 01-09 المادة 389، المؤرخ في 25 فبراير 2009 المعدل والمتمم للأمر 66-156 المؤرخ 8 يونيو 1966، المتضمن قانون العقوبات ج ر، العدد 15، 2009.

⁴ القانون رقم 01-09 المادة 389، المؤرخ في 25 فبراير 2009 المعدل والمتمم للأمر 66-156 المؤرخ 8 يونيو 1966، المتضمن قانون العقوبات ج ر، العدد 15، 2009.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

. الحرمان من ممارسة الحقوق الوطنية والمدنية والعائلية.

. تحديد الإقامة .المنع من الإقامة.

. المصادرة الجزئية للأموال.

. المنع المؤقت من ممارسة مهنة أو نشاط.

. إغلاق مؤسسة.

. الإقصاء من الصفقات.

. الحظر من إصدار الشيكات و/أو استعمال وسائل الدفع

. تعليق أو سحب رخصة السياقة أو إلغاؤها مع المنع من استصدار رخصة جديدة

. سحب جواز السفر.

. نشر أو تعليق حكم أو قرار الإدانة.

أما بالنسبة للشخص المعنوي فقد نصت المادة 389 مكرر 7 أن عقوبته تتمثل في 4 مرات من الغرامة المحددة سابقاً في المادتين 389 مكرر 1 و 389 مكرر 2، بالإضافة إلى مصادرة الممتلكات والعائدات والوسائل المستعملة في الجريمة، بالإضافة إلى عقوبتين تكميليتين وهما إما المنع من مزاوله النشاط لمدة لا تفوق 5 سنوات أو حل الشخص الاعتباري¹.

من خلال تحليل للمواد السابقة المتعلقة بقانون العقوبات نستنتج أن المشرع الجزائري عاقب على الشروع في ارتكاب جريمة تبييض الأموال واصراره على مكافحتها.

2. قانون الإجراءات الجزائية:

استحدث المشرع الجزائري بموجب قانون الإجراءات الجزائية مجموعة من الإجراءات الخاصة التي لمواكبة الجرائم المرتبطة بالعالم التكنولوجي مع استحداث طرق جديدة للتحري والتحقيق المتعلقة بهذه الجريمة منها ما شمل صلاحيات ضباط الشرطة القضائية² وتتمثل في: اعتراض المراسلات والتقاط الصور وتسجيل الأصوات؛ وإجراء التسرب، حيث سمح المشرع الجزائري باللجوء إلى اعتراض المراسلات والتقاط الصور

¹ القانون رقم 09-01 المادة 389، المؤرخ في 25 فبراير 2009 المعدل والمتمم للأمر 66-156 المؤرخ 8 يونيو 1966، المتضمن قانون العقوبات ج ر، العدد 15، 2009.

² ناجية شيخ، أساليب البحث والتحري المستحدثة في القانون رقم 06.22 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري، المجلة النقدية، جامعة مولود معمري، تيزي وزو، العدد 1، 2013، ص 279.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

وتسجيل الأصوات خاصة في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات؛ مع إلزام احترام سرية المراسلات والضمانات القانونية.

وأشار المشرع بموجب المادة الثالثة من القانون 04-09 إلى ضرورة احترام سرية المراسلات، وعرف الاتصالات الإلكترونية في المادة الأولى من نفس القانون بأنها: أي ترسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة لأي رسالة إلكترونية¹. وكإجراء آخر فقد أجاز المشرع اللجوء إلى التسرب بموجب المادة 65 مكرر 11 قانون الإجراءات الجزائية، إذا اقتضت ضرورة التحري والتحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، حيث يجوز لوكيل الجمهورية أو لقاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب باحترام الضمانات والشروط المقررة قانوناً والمتمثلة في احترام شرط الإذن المكتوب والمسبب ومن ثم لا يمكن استخدام هوية مستعارة للقيام بالتسرب في مدة زمنية محددة تقدر بأربعة أشهر قابلة للتجديد، ويحرر تقريراً يتضمن أهم العناصر الضرورية لمعينة الجريمة².

3- قانون رقم 04-09 المؤرخ في 5 / 8 / 2009³:

لم ينص هذا القانون صراحة على جريمة تبييض الأموال، وإنما هو يتعلق بالجرائم المعلوماتية، حيث عرف الإلكترونية في المادة الثانية من هذا القانون على أنها: "كل جريمة متصلة بأنظمة المعالجة للمعلومات أو كان الحاسوب جزء من الجريمة"⁴ وباعتبار أن جريمة تبييض الأموال، يقوم أساسها على الأنظمة المعلوماتية والحواسيب، يمكن هنا التوصل إلى اعتبارها جريمة الكترونية وتخضع لقواعد قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

¹ القانون رقم 04-09، المادة 3، المؤرخ بتاريخ 5 أوت 2009، المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر، العدد 47، 2009.

² جمال براهيم، مكافحة الجريمة الإلكترونية في التشريع الجزائري، المجلة النقدية للقانون والعلوم السياسية، جامعة مولود معمري، تيزي وزو، العدد 2، 2016، ص 124.

³ القانون رقم 04-09، المادة 3، المؤرخ بتاريخ 5 أوت 2009، المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر، العدد 47، 2009.

⁴ القانون رقم 04-09، المادة 3، المؤرخ بتاريخ 5 أوت 2009، المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر، العدد 47، 2009.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

ولقد جاء في القانون 09-04 المؤرخ في 5/8/2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها،⁴⁷ الذي يحتوي على 6 فصول تناولت التعريف بالجريمة ومراقبة الاتصالات الإلكترونية، القواعد الإجرائية، الهيئة الوطنية للوقاية من الجرائم المعلوماتية والاختصاص القضائي وهذا في 19 مادة بوضعه مجموعة من التدابير الوقائية التي يتم اتخاذها مسبقاً من طرف مصالح معينة لتفادي وقوع جرائم معلوماتية أو الكشف عنها وعن مرتكبيها في وقت مبكر، وهي كالتالي:

أ- مراقبة الاتصالات الإلكترونية: لقد نصت المادة 04 من القانون 09-04 على أربع حالات التي يجوز فيها لسلطات الأمن القيام بمراقبة المراسلات والاتصالات الإلكترونية، وذلك بالنظر إلى خطورة التهديدات المحتملة وأهمية المصلحة المحمية وهي :

- . للوقاية من الأفعال التي تحمل وصف جرائم الإرهاب والتخريب وجرائم ضد أمن الدولة.
- . عندما تتوفر معلومات عن احتمال وقوع اعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو النظام العام.
- . لضرورة التحقيقات والمعلومات القضائية حينما يصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.
- . في إطار تنفيذ طلبات المساعدات القضائية الدولية المتبادلة.

ب- إقحام مزودي خدمات الاتصالات الإلكترونية في مسار الوقاية من الجرائم المعلوماتية: وذلك من خلال فرض عليهم مجموعة من الالتزامات مذكورة في المواد 10، 11، 12 وذلك بـ:

- . الالتزام بالتعاون مع مصالح الأمن المكلف بالتحقيق القضائي عن طريق جمع أو تسجيل المعطيات المتعلقة بالاتصالات والمراسلات ووضعها تحت تصرفها مع مراعاة سرية هذه الإجراءات والتحقيقات.
- . الالتزام بحفظ المعطيات المتعلقة بحركة السير وكل المعلومات التي من شأنها أن تساهم في الكشف عن الجرائم ومرتكبيها¹.

¹ القانون رقم 09-04، المادة 3، المؤرخ بتاريخ 5 أوت 2009، المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر، العدد 47، 2009

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

4. قانون مكافحة التهريب:

يعد التهريب من أبرز الأساليب الأساسية التي يستعملها مبيضي الأموال في عملياتهم، سواء لإخفاء المال القذر المتحصل عليه عن طريق تهريبه، وعليه نص قانون محاربة التهريب جملة من التدابير، لمحاربة تبييض الأموال، كإنشاء الديوان الوطني لمكافحة التهريب، كما أقر بإجراءات ردعية صارمة¹.

وهو من الجرائم التي عرفت تطوراً ملحوظاً بفعل التحول الرقمي، حيث لم يعد يقتصر على الطرق التقليدية في نقل الأموال والسلع، بل أصبح يعتمد على وسائل إلكترونية حديثة كمنصات التجارة الرقمية والتحويلات المالية الإلكترونية والعملات الافتراضية، الأمر الذي جعله مرتبطاً بصورة مباشرة بجريمة تبييض الأموال في البيئة الرقمية

وفي هذا الإطار، تدخل المشرع الجزائري في المادة الأولى من خلال القانون رقم 05-06 المتعلق بمكافحة التهريب، المعدل والمتمم²، بهدف الحد من مختلف صور التهريب التي تشكل مصدراً للعائدات غير المشروعة القابلة للتبييض وقد تضمن هذا القانون مجموعة من التدابير الوقائية والإجراءات الردعية، من بينها تعزيز الرقابة الجمركية على حركة الأموال والسلع عبر الحدود، وتوسيع صلاحيات أعوان الجمارك في المعاينة والتفتيش والحجز، إضافة إلى مصادرة الوسائل والعائدات المستعملة أو الناتجة عن جريمة التهريب

كما أقر عقوبات مشددة ضد الأفعال المرتكبة في إطار جماعات إجرامية منظمة، خاصة إذا ارتبطت بعمليات مالية مشبوهة أو استعملت فيها وسائل تقنية حديثة تهدف إلى إخفاء المصدر غير المشروع للأموال، وهو ما يعكس سعي المشرع إلى مواكبة التطور الرقمي للجرائم المالية وتعزيز آليات مكافحة تبييض الأموال في البيئة الرقمية.

ثانياً: الهيئات الوطنية المكلفة بمكافحة جريمة تبييض الأموال في البيئة الرقمية

خصص المشرع الوطني مؤسسات ومصالح ووحدات من أجل مكافحة جريمة تبييض الأموال، فعلى المستوى الوطني في الجزائر مثلاً نجد: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام

¹ سعيد فروحات، الإجراءات الوقائية والقلمية لمكافحة تبييض الأموال في الجزائر، مجلة الواحات للبحوث والدراسات، جامعة غرداية، العدد 1، 2015، ص 349.

² القانون رقم 05-06، المادة 1، المؤرخ في 23 أوت 2005، المتعلق بمكافحة التهريب، ج ر، العدد 59، الصادر بتاريخ 28 أوت 2005، المعدل والمتمم.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

والاتصال ومكافحتها والمصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني، ومركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية التابع للدرك الوطني وكذا المعهد الوطني للأدلة الجنائية وعلم الإجرام التابع هو الآخر للدرك الوطني فعمد للبحث عن وسائل أخرى أكثر فعالية للحد من هذه الجريمة أو على الأقل التقليل من انتشارها¹ خصوصاً بما تعلق بالاقتصاد².

1- خلية معالجة الاستعلام المالي:

خرج الاجتماع الذي عقده مجلس الأمن الدولي في 28 سبتمبر 2001 عقب أحداث 11 سبتمبر 2001 التي هزت الولايات المتحدة الأمريكية بالعديد من التوصيات، من بينها وجوب إنشاء هيئة متخصصة بالاستعلام المالي على مستوى كل دولة ذات مهام متعددة في مجال مكافحة الفساد والجرائم ذات الخطورة البالغة من بينها جريمة تبييض الأموال، واستجابة لذلك قامت الجزائر بإنشاء خلية معالجة الاستعلام المالي (cellule de traitement du renseignement financier) بموجب المرسوم التنفيذي رقم 02-127 المؤرخ في 07 أبريل 2002، وتم تنصيبها الفعلي في سنة 2004³.

أ- هيكلية خلية معالجة الاستعلام المالي:

تعد خلية معالجة الاستعلام المالي مؤسسة عمومية تتمتع بالشخصية المعنوية والاستقلال المالي، مقرها الجزائر العاصمة، تتكون من 6 أعضاء من بينها الرئيس، ينتقون حسب كفاءتهم في المجالات المصرفية والمالية والأمنية، ويعينون بموجب مرسوم رئاسي لعهد مدتها أربع (04) سنوات قابلة للتجديد مرة واحدة

ب- مهام خلية معالجة الاستعلام المالي:

طبقاً للمادة الرابعة من المرسوم التنفيذي 02-127 المؤرخ في 7 أبريل 2002 المعدل والمتم للمرسوم التنفيذي الجديد رقم 22-36 المؤرخ 4 جانفي 2022 المتعلق بمهام خلية معالجة الاستعلام المالي هي⁴:

¹ أمانة تازير، جريمة تبييض الأموال في التشريع الجزائري بين القمع والوقاية، مجلة دراسات إنسانية واجتماعية، جامعة وهران 3، العدد 10، جوان 2019، ص 300.

² ارتباس نذير، طارق قادري، الجريمة الالكترونية وحجية الدليل الرقمي في الاثبات الجنائي، المركز المغربي، ط1، جانفي 2024، ص 399.

³ أمانة تازير، مرجع سابق، ص 300.

⁴ المرسوم التنفيذي رقم 22-36، المادة 4، المؤرخ في 4 جانفي 2022، الذي يحدد مهام خلية معالجة الاستعلام المالي وتنظيمها وسيرها، ج ر، العدد 03، 2022.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

- تسلم تصريحات الاشتباه المتعلقة بكل عمليات غسيل الأموال أو تمويل الإرهاب
- إرسال الملف لوكيل الجمهورية المختص طبقاً للقانون في كل مرة يحتمل فيها أن تكون الوقائع المصرح بها مرتبطة بجريمة غسيل الأموال أو تمويل الإرهاب . اقترح النصوص التشريعية والتنظيمية والتي يكون موضوعها مكافحة غسيل الأموال
- الاعتراض بصفة تحفظية ولمدة أقصاها 72 ساعة على تنفيذ أي عملية مصرفية لأي شخص طبيعي أو معنوي تقع عليه شبهة قوية لغسيل الأموال .
- حجز كل الأموال غير المشروعة المتحصلة من جريمة تبييض الأموال¹.

ولها في سبيل إنجاز هذه المهام أن تطلب أية وثيقة أو أية معلومة ضرورية من الهيئات والأشخاص الذين يعينهم القانون، كما لها أن تستعين بأي شخص مؤهل لمساعدتها على تأدية مهامها

2 - السلطة العليا للشفافية والوقاية من الفساد ومكافحته:

يعد قانون الوقاية من الفساد ومكافحته من أبرز القوانين التي ساهمت في تعزيز آليات مكافحة تبييض الأموال، إذ تضمن تدابير وقائية ورقابية تهدف إلى تعزيز الشفافية والكشف عن الأموال غير المشروعة، كما تم تدعيم هذه الآليات بموجب القانون رقم 08-22 المتعلق بالسلطة العليا للشفافية والوقاية من الفساد ومكافحته في المادة الرابعة منه².

أ- هيكلية السلطة العليا للشفافية والوقاية من الفساد ومكافحته:

تتشكل هذه الهيئة من رئيس وستة أعضاء، يعينون بموجب مرسوم رئاسي لمدة خمس (5) سنوات قابلة للتجديد مرة واحدة فقط، وهذه الهيئة مقسمة إلى 03 أقسام: مجلس اليقظة والتقييم - مديرية الوقاية والتحسيس - مديرية التحاليل والتحقيقات³.

¹ يزيد بوحليط، السياسة الجنائية في مجال تبييض الأموال في الجزائر، د ط، دار الجامعة الجديدة، الجزائر، 2014، ص 234.

² قانون رقم 8-22، المادة 4، المؤرخ في 5 ماي 2022، المعدل والمتمم لقانون 01-06 المؤرخ 20 فيفري 2006، المتعلق بالوقاية من الفساد ومكافحته، ج ر، العدد 32، 2022.

³ قانون رقم 8-22، المادة 4، المؤرخ في 5 ماي 2022، المعدل والمتمم لقانون 01-06 المؤرخ 20 فيفري 2006، المتعلق بالوقاية من الفساد ومكافحته، ج ر، العدد 32، 2022.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

ب- مهام السلطة العليا للشفافية والوقاية من الفساد ومكافحته:

بعد التعديل الذي جاء به القانون رقم 22-08 المؤرخ في 5 ماي 2022، تم استبدال الهيئة الوطنية للوقاية من الفساد ومكافحته بالسلطة العليا للشفافية والوقاية من الفساد ومكافحته، والتي أوكلت لها مهام أوسع في مجال الوقاية من الفساد وتعزيز الشفافية، وهي تنحصر فيما يأتي:

- . اقتراح سياسة شاملة للوقاية من الفساد.
- . تقديم توجيهات تخص الوقاية من الفساد لكل شخص أو هيئة عمومية أو خاصة.
- . إعداد برنامج بتوعية وتحسيس المواطنين بالآثار الضارة والناجمة عن الفساد.
- . جمع واستغلال كل المعلومات التي تساهم في الكشف عن أعمال الفساد والوقاية منها .
- . التقييم الدولي للأدوات القانونية والإجراءات الإدارية الرامية إلى الوقاية من الفساد ومكافحته.
- . تلقي التصريحات بالامتلاكات الخاصة بالموظفين العموميين بصفة دورية .
- . الاستعانة بالنيابة العامة لجمع الأدلة والتحري في وقائع ذات علاقة بالفساد.
- . ضمان تنسيق ومتابعة النشاطات والأعمال المباشرة ميدانياً .
- . السهر على تعزيز التنسيق بين القطاعات وعلى التعاون مع هيئات مكافحة الفساد على الصعيد الوطني والدولي، والحث على كل نشاط يتعلق بالبحث عن الأعمال المباشرة في مجال الوقاية من الفساد ومكافحته وتقييمها¹.

بالإضافة إلى قانون الفساد كان للشرطة القضائية دور فعال في محاربة جريمة تبييض الأموال في البيئة الرقمية، من خلال عدة إجراءات كالبحث والتحري، التسليم المراقب، التسرب، التردد الإلكتروني.

أساليب التحري الخاصة بالشرطة القضائية:

نصت مواد قانون الفساد 06-01، على إمكانية استعمال أساليب تحري خاصة لجمع الأدلة حول الجرائم، والمقصود بهذه الأساليب هي تلك الإجراءات والطرق، التي تستعملها الشرطة القضائية تحت إشراف السلطة القضائية المخولة، للكشف والتحري عن جريمة تبييض الأموال في البيئة الرقمية، وكذلك الإلمام بكل الأدلة عن الواقعة دون علم مرتكبيها² ومن هذه الأساليب:

التسليم المراقب:

¹ القانون رقم 06-01، المادة 56، المؤرخ في 20 فبراير 2006، المتعلق بالوقاية من الفساد ومكافحته، ج ر، العدد 14، 2006.

² نصر الشريف العربي، أساليب التحري في جرائم الفساد، دراسات الوظيفة العامة، المركز الجامعي نور البشير، البيض، العدد 4، 2017، ص 148.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

عرف قانون الفساد أسلوب التسليم المراقب في المادة الثانية منه بأنه: السماح بدخول مضبوطات أو أموال غير مشروعة، أو خروجها من الإقليم الوطني تحت مراقبة السلطات المختصة وعلمها. بهدف الكشف عن الجرائم المرتبطة بتبييض الأموال والوصول إلى الأشخاص المتورطين فيها، ويخضع التسليم المراقب لعدة ضوابط قانونية، حيث يجب الحصول على إذن من وكيل الجمهورية المختص، وهذا بموجب المادة 6 من قانون الإجراءات الجزائية 06-101¹.

الترصد الإلكتروني:

الترصد الإلكتروني هو مراقبة منتظمة ومستمرة للأشخاص المشتبه في تورطهم في جريمة تبييض الأموال في البيئة الرقمية، قبل ارتكاب الجريمة، أو أثناءها، أو بعدها، باستعمال الوسائل الإلكترونية الحديثة لرصد نشاطه وتوثيق ذلك في محاضر رسمية².

نظام التسرب:

يقصد بالتسرب هو السماح لعون الشرطة القضائية، الدخول داخل مجموعة إجرامية مشتبه في تورطها في جريمة تبييض الأموال في البيئة الرقمية تحت مسؤولية ضابط شرطة قضائية مختص بهدف مراقبة الأشخاص المشتبه فيهم وكشف أنشطتهم الإجرامية بطريقة غير مباشرة عن طريق التخفي، والتعامل معهم كفاعل أصلي أو شريك في الجريمة³.

حددت المادة 65 مكرر 12 من قانون الإجراءات الجزائية 3 صور لعملية التسرب حيث يكون المخترق إما المتسرب كفاعل: يأخذ الضابط صفة الفاعل الرئيسي في العملية أو يكون المتسرب كشريك: أي لا يكون فاعل أصلي وإنما مساعد فقط يسهل ارتكاب الجريمة⁴، وقد يكون المتسرب كخاف: يُسمح للمتسرب القيام بإخفاء أشياء تخص متعلقات الجريمة عمداً بهدف حمايته وعدم كشفه⁵.

¹ القانون رقم 06-01، المادة 6، المؤرخ في 20 فبراير 2006، المتعلق بالوقاية من الفساد ومكافحته، ج ر، العدد 14، 2006.

² عثمان خرشي، الترصد الإلكتروني كآلية لمكافحة الجرائم المعلوماتية، مجلة الدراسات الحقوقية، جامعة الطاهر مولاي، سعيدة، العدد 3، 2020، ص 804.

³ هدى زوزو، التسرب كأسلوب من أساليب التحري في القانون الإجراءات الجزائية الجزائري، مجلة دفاتر السياسية والقانون، جامعة قاصدي مرباح، ورقلة، العدد 11، 2014، ص 117.

⁴ أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، ج 2، ط 10، دار الهومة، الجزائر، 2008، ص 42.

⁵ صالح شنين، التسرب في قانون الإجراءات الجنائية الجزائري حماية للنظام العام والحريات أم حماية للنظام العام، المجلة الجزائرية للقانون المقارن، جامعة أبو بكر بلقايد، تلمسان، العدد 2، 2015، ص 122.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

3-الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها:

أنشئت هذه الهيئة بموجب القانون رقم 09-04 المؤرخ في 5 أوت 2009 والذي حددت المادة 14 منه مهام الهيئة في مكافحة جريمة تبييض الأموال والمتمثلة في:

- . تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.
- . مساعدة السلطات القضائية ومصالح الشرطة القضائية في المحققة في الجريمة من خلال جمعها للمعلومات وإنجاز الخبرات القضائية.
- . تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة.
- . في التعرف على مرتكبي الجرائم تبييض الأموال في البيئة الرقمية وتحديد مكان تواجدهم.

4-المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني:

يعتبر الدرك الوطني من الأسلاك الأمنية المهمة لمكافحة جريمة تبييض الأموال عبر الوسائل الرقمية، وقد كان المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني من الأجهزة والمراكز للقيام بهذه المهمة.

أنشئ هذا المعهد بموجب مرسوم رئاسي رقم 04-183 المؤرخ في 27 جوان 2004 مقره الجزائر العاصمة بوشاوي، وهو مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلال المالي، ويوضع تحت وصاية وزير الدفاع الوطني، يتكون المعهد من 11 دائرة متخصصة في مجالات مختلفة من بينها دائرة الإعلام الآلي والإلكتروني مكلفة بمعالجة وتحليل وتقديم كل دليل رقمي يساعد العدالة كما تقدم مساعدة تقنية للمحققين في المعاينات لجريمة¹، ومن أهم وظائفه مكافحة جميع الجرائم الإلكترونية بما فيها تبييض الأموال الرقمي عن طريق البحث و التحري بقسم الإعلام الآلي والإلكتروني²

¹ أمانة تازير، مرجع سابق، ص300

² سعيدة بوزنون، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة العلوم الإنسانية، جامعة محمد خيضر، بسكرة، العدد3، 2019، ص53.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

5-مركز الوقاية من جرائم الإعلام الآلي والجرائم الإلكترونية:

تم إنشاء هذا المركز بموجب مرسوم رئاسي 08-44، المؤرخ في 9 فبراير 2008، المتضمن إنشاء مركز الوقاية من الجرائم الإعلام الآلي والاتصال وتحديد مهامه وتنظيمه¹، مقره الجزائر العاصمة - بئر مراد رابس، يعتبر كذلك من الأجهزة التي يستعين بها الدرك الوطني في محاربة جرائم تبييض الأموال في البيئة الرقمية المنصوص عليها في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها 09-04²

كما يهدف هذا المركز إلى مساعدة باقي الأجهزة الأخرى في أداء المهام التالية³:

-ضمان المراقبة الدائمة والمستمرة على شبكة الأنترنت.

-القيام بمراقبة الاتصالات الإلكترونية بما يسمح به القانون لفائدة وحدات الدرك الوطني.

- المساعدة بالمعينة في الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال والبحث عن الأدلة.

- المشاركة في عمليات التحري والتسرب عبر شبكة الأنترنت.

- المشاركة في قمع الجرائم المعلوماتية.

6- بنك الجزائر:

يبرز دور بنك الجزائر كسلطة نقدية ورقابية في تعزيز منظومة الوقاية والمكافحة، وقد جاء النظام رقم 25-14 المؤرخ في 24 سبتمبر 2025، المعدل والمتمم للنظام 24-03⁴ في المادة الأولى منه ليعكس هذا التوجه من خلال تدعيم آليات الرقابة الداخلية داخل البنوك والمؤسسات المالية، وتطوير إجراءات

¹ المرسوم الرئاسي رقم 08-44، المؤرخ في 9 فبراير 2008، المتضمن إنشاء مركز الوقاية من الجرائم الإعلام الآلي والاتصال وتحديد مهامه وتنظيمه، ج ر، العدد 8، 2008.

² عبد القادر فلاح، نادية آيت عبد المالك، التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، المسيلة، العدد 2، 2019، ص 1696.

³ سعاد رابح، ضوابط مكافحة الجريمة المعلوماتية، مجلة القانون العام الجزائري والمقارن، جامعة الجيلالي الياصب، سيدي بلعباس، العدد 1، 2021، ص 281.

⁴ النظام رقم 25-14، المادة 1، المؤرخ في 24 سبتمبر 2025، يعدل ويتمم النظام رقم 24-03 المؤرخ في 24 يوليو 2024، المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب وتمويل انتشار أسلحة الدمار الشامل ومكافحتها، ج ر، العدد 68، 2025.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

اليقظة والإبلاغ عن العمليات المشبوهة، بما يتماشى مع متطلبات البيئة الرقمية الحديثة ويعزز حماية النظام المالي الوطني.

يمكن تلخيص دور بنك الجزائر في هذا الإطار عبر النقاط التالية:

-توسيع نطاق المؤسسات الخاضعة للرقابة ليشمل مزودي خدمات الدفع حيث قام بنك الجزائر بتوسيع مفهوم "المؤسسة الخاضعة" لتشمل بشكل صريح مزودي خدمات الدفع مما يعني أن الجهات الفاعلة في البيئة الرقمية أصبحت ملزمة الآن بوضع وتنفيذ برامج رقابة داخلية وتدابير عناية واجبة للوقاية من تبييض الأموال.

- تدابير صارمة تجاه الأصول الافتراضية (Virtual Assets) :

_فرض النظام الجديد قيوداً تقنية وإجرائية مشددة للتعامل مع المخاطر المرتبطة بالقيم الرقمية

-المنع الآلي: يُلزم النظام المؤسسات الخاضعة بوضع نظام آلي وفعال يسمح بالمنع والتوقيف الفوري لأي عملية مرتبطة بالأصول الافتراضية أو بمزودي خدماتها، خاصة تلك المنشأة خارج الجزائر.

-إلزام المؤسسات المالية بالإخطار الفوري للجهات المختصة (خلية معالجة الاستعلام المالي) بكل عملية مشبوهة تتعلق بالأصول الافتراضية.

- تحديد المفاهيم وضح النظام أن "الأصول الافتراضية" لا تشمل القيم الرقمية للعملات الورقية أو الأوراق المالية أو غيرها من الأصول المالية التقليدية.

-تعزيز الرقابة على علاقات المراسلة البنكية.

-سياق التعاملات المالية الدولية التي تتم غالباً عبر القنوات الرقمية، شدد النظام على تدابير العناية الواجبة عند التعامل مع مؤسسات مالية أجنبية يجب على المؤسسات التأكد من أن المؤسسات المستجيبة قد طبقت تدابير العناية الواجبة تجاه زبائنهم الذين يملكون وصولاً مباشراً إلى حسابات المراسلة.

- تعزيز تدابير العناية الواجبة في علاقات المراسلة البنكية، مع منع التعامل مع البنوك الصورية

(Shell Banks) التي لا تملك وجوداً فعلياً في بلد تأسيسها

-تطبيق مبدأ التناسبية والمخاطر: أقر بنك الجزائر ضرورة مراعاة مبدأ التناسبية عند تطبيق هذه الأحكام على مكاتب الصرف ومزودي خدمات الدفع، مع الأخذ في الاعتبار طبيعة أنشطتهم، حجمهم،

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

والمخاطر المرتبطة بهم في البيئة الرقمية تُظهر هذه التعديلات توجه بنك الجزائر نحو عولمة الرقابة الرقمية من خلال فرض أنظمة آلية للمراقبة، وتوسيع دائرة الخاضعين للرقابة لتشمل المبتكرين في مجال الخدمات المالية الرقمية.

الفرع الثاني

التدابير الوقائية

بذلت الجزائر تحديثاً لترسانتها القانونية عبر قوانين خاصة وإنشاء هيئات أمنية متخصصة للتحري، وهو ما يظهر جلياً من خلال تبني مجموعة من الوسائل والأدوات القانونية، منها ما يخص الجانب المصرفي الذي اعتبره المجرمون ملاذهم في تنفيذ جرائمهم، ومنها ما يخص الجانب المعلوماتي باعتباره جزءاً من الجريمة، وهذا ما سنعرضه لاحقاً، حول التحقيقات حول الحسابات البنكية (أولاً) وجوب تطوير أنظمة الحماية الإلكترونية لمكافحة جريمة تبييض الأموال في البيئة الرقمية (ثانياً) وحظر التعامل بالأصول الافتراضية كآلية وقائية لمكافحة تبييض الأموال في البيئة الرقمية (ثالثاً).

أولاً: التحقيقات حول الحسابات البنكية

للحد من عمليات تبييض الأموال، يجب على البنوك أن يكون لها دور فعال في هذه العملية، وتماشياً مع التوصية العاشرة التي أوصت بها مجموعة العمل المالي في توصياتها الأربعون¹.

1. التحقق من هوية الزبون:

عملاً كذلك بالتوصية 12 من مجموعة العمل المالي الدولية، فإنه يتوجب على البنوك التحقق من هوية الزبون المحتمل، سواء كان شخصاً طبيعياً عن طريق جملة من الوثائق القانونية، ويتم تسجيلها على أجهزة الحاسوب لذات البنك، وإذا كان الشخص اعتبارياً فيتولى البنك مهمة التحقيق والوجود الفعلي لهذا الكيان، عن طريق السجلات التجارية والمستندات القانونية الأصلية لهذه الشركة².

وهذا ما أكدته قانون 01-05 في مواده، حيث أنه يجب التأكد من حقيقة الزبائن سواء كانوا طبيعيين أو معنويين³، وبالرجوع لمواد النظام 12-03 أكدت على وجوبية التأكد الصحيح من هوية الأشخاص

¹ نهلة قيوم، بريق وصال درة القدس، جريمة تبييض الأموال باستخدام الوسائط الإلكترونية، مذكرة مقدمة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة محمد الشريف مساعدي، سوق اهراس، 2023، ص28

² المرجع نفسه، ص28.

³ الأمر رقم 01-05، المادة 7، المؤرخ في 06 فيفري 2005، المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتها، ج ر، العدد 11، 2005.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

الطبيعيين عن طريق الوثائق الرسمية المرفقة بصورة شخصية، أما الأشخاص المعنويين عن طريق القوانين الأصلية وسندات الإنشاء أو أوراق الاعتماد القانونية للشركات والكيانات المراد فتح حسابات لها¹.

كذلك نص القانون السابق في المادة 7، أنه يجب على البنك التحقق من هوية الوسطاء الذين يعملون لحساب الغير وإعطاء وثائق ثبوتية للمستفيدين الحقيقيين².

فقام المشرع الجزائري في تعديل 02-12 لقانون الوقاية من تبييض الأموال، إلى وضع تعريف دقيق للمستفيد الحقيقي حيث نصت المادة الثانية من الأمر 02-12 التي تعدل المادة الرابعة من القانون 05-01 على أنه: "الشخص أو الأشخاص الطبيعيون الذين يملكون أو يمارسون سيطرة فعلية في النهاية على الزبون و/أو الشخص الذي تتم العمليات نيابة عنه كما يتضمن أيضاً الأشخاص الذين يمارسون سيطرة فعلية نهائية على شخص معنوي".

وقد أكدت المادة 6 المعدلة للمادة 9 بالأمر 02-12 على عبارة المستفيد الحقيقي، وأكدت أيضاً أنه يجب على البنك القيام بجميع التحريات الخاصة للتأكد من هوية العميل مهما كانت صفته³ لقد أفادت كذلك مبادئ ولفسبيرج لمكافحة غسيل الأموال، أنه يتوجب على البنوك القيام بتحديث ملفات العملاء، وهذا ما قام به المشرع الجزائري بالمشي نحوه ونص عليه في المادة السبعة من قانون 05-01 المعدل والمتمم السالف الذكر.

2. تدريب موظفي البنك:

يجب على البنوك تكوين موظفيها، وإرسالهم لدورات تدريبية خاصة، لاكتشاف السلوكات المالية المشبوهة، عن طريق طرح أسئلة للتجار، أو استعمال برنامج المتابعة الحركية الفورية (monitoring) للبطاقات الائتمانية للتجار، عند سحبهم لمبالغ مالية أكثر من المعتاد والتنسيق مع المحلات التجارية التي اعتاد التجار التعامل معها، من أجل تسهيل عملية الكشف عن الأموال المشبوهة⁴.

¹ نظام رقم 03-12، المادة 5، المؤرخ في 2012/11/28، المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهم، ج ر، العدد 12، 2013.

² الامر رقم 01-05، المادة 5، المؤرخ في 06 فيفري 2005، المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهم، ج ر، العدد 11، 2005.

³ الامر رقم 02-12، المادة 6، المؤرخ في 2012/2/13، يعدل ويتم القانون رقم 01-05، المادة 9، المؤرخ في 2005/2/6، المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب، ومكافحتهم، ج ر، العدد 8، 2012.

⁴ نهلة قيوم، بريق وصال درة القدس، مرجع سابق، ص 29.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

وقد أكد المشرع الجزائري على إلزامية تأهيل وتكوين الموظفين في القطاع البنكي، من خلال الأمر 02-12 المعدل والمتمم لقانون الوقاية من تبييض الأموال¹.

كذلك نص النظام البنكي رقم 03-12 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب، على ضرورة وضع برنامج تدريب للموظفين، لمعرفة كل العمليات التي يقومون بها، وكذلك يتعرفون على أساليب تبييض الأموال خاصة التي تعتمد الأساليب الحديثة²

ثانيا: وجوب تطوير أنظمة الحماية الإلكترونية لمكافحة جريمة تبييض الأموال في البيئة الرقمية
بشكل فعال خاصة في الصورة الحديثة لها باستعمال البيئة الرقمية، كان من الواجب استعمال أفضل التطبيقات والأنظمة للحماية من هذه الجريمة المالية.

1 . استخدام نظام OMNIEntreprise

وهو يعتبر نظام معلوماتي من إنتاج بنك الخليج والشركة العالمية للبرمجيات IMTAC ، حيث صمم هذا البرنامج للحماية من العمليات المشبوهة لتبييض الأموال، عن طريق مجموعة أساليب تكشف المعاملات المشبوهة، كذلك تقوم بتقسيم معاملات الزبائن، ومن هنا تقوم بإرسال تحذيرات للبنك حول المسائل المشكوك فيها.

2 . تقنية التشفير:

ويقصد بالتشفير تبديل المعلومات إلى أرقام ورموز، لا يستطيع أي كان قراءتها، إلا عن طريق مفاتيح الكود لفك التشفير، وتصبح مفهومة³
ويعتبر التشفير كأحد الأنظمة الرقمية، لحماية المعاملات المصرفية الرقمية، وتعتبر أحد آليات حماية وسائل الدفع ضد مخاطر الجرائم المرتكبة عليها، كالتزوير، أو الاستيلاء على المعطيات السرية وعمليات

¹ الامر رقم 02-12، المادة 10، المؤرخ 2012/2/13، يعدل ويتم القانون رقم 05-01، المادة 9، المؤرخ في 2005/2/6، المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب، ومكافحتهما، ج ر، العدد 8، 2012.

² نظام رقم 03-12، المادة 18، المؤرخ في 2012/11/28، المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، ج ر، العدد 12، 2013.

³ فتيحة يوسف، هداية بوعزة، الحماية التقنية للمعلومات ودورها في تأمين نظام الدفع الإلكتروني، مجلة الدراسات والبحوث القانونية، جامعة محمد بوضياف، المسيلة، العدد 4، 2018، ص 30.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

تحويل الأموال .كذلك عن طريق تقنية التشفير، يمكننا تجنب جملة من المخاطر، أهمها انتحال شخصية المستخدم الحقيقي، محاولة تعديل البيانات إلى جهة أخرى، الاطلاع على المعلومات الشخصية والسرية¹.

3 . استخدام بروتوكولات الحماية:

من أشهر البروتوكولات SSL, TLS التي تستخدمها البنوك والمصارف لحماية الاتصالات الخالية من الخطر، ونقل المستندات بصفة آمنة عن طريق الإنترنت، أي أنهما يضمنان الخصوصية ودقة البيانات، فهما يقومان على التأكد من المستخدم الحقيقي وأنه المالك الشرعي للحساب، كما يسهلان التعرف بين الخادم والتابع للاتصال دون شيفرة².

4 . تقنية الحوائط النارية Pare-feu :

تعتبر تقنية الحوائط النارية تقنية مبتكرة لتأمين الشبكات التي يتم الاتصال فيها عن طريق الإنترنت، إذ يعتبر نظام حماية للحاسوب من الاعتداءات التي يمكن أن يتعرضها كالتجسس، من خلاله لا يمكن السماح للأفراد غير المرخص لهم بمعرفة المعلومات والبيانات السرية والشخصية كأرقام بطاقات الائتمان³. نستنتج من خلال ما سبق أن لمكافحة جريمة تبييض الأموال في البيئة الرقمية لابد من استعمال أفضل الأنظمة للحماية من هذه الجريمة.

ثالثاً: حظر التعامل بالأصول الافتراضية كآلية وقائية لمكافحة تبييض الأموال في البيئة الرقمية

في إطار تعزيز التدابير الوقائية لمكافحة تبييض الأموال في البيئة الرقمية، جاء القانون رقم 10-25 المعدل والمتمم للقانون رقم 01-05 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، ليكرّس حظر التعامل بالأصول الافتراضية.

وقد عرّف الأصول الافتراضية بأنها: قيم رقمية يمكن تداولها أو تحويلها رقمياً واستعمالها لأغراض الدفع أو الاستثمار، كما منع إصدارها أو بيعها أو شرائها أو حيازتها أو الترويج لها أو إنشاء منصات لتداولها، نظراً لما قد تشكله من مخاطر في مجال تبييض الأموال وتمويل الإرهاب⁴.

¹ عبد الرؤوف دباش، هشام ذبيح، وسائل الدفع مابين الحماية التقنية والقانونية للمستهلك الإلكتروني، مخبر أثر الاجتهاد القضائي على حركة التشريع، جامعة محمد خيضر، بسكرة، العدد14، 2014، ص108.

² محمد شايب، نعيمة برك، الوقاية من تزوير بطاقات الدفع الإلكترونية كآلية للحد من الفساد المالي في البنوك والمؤسسات المالية، مجلة دفاتر اقتصادية، جامعة زيان عاشور، الجلفة، العدد1، 2011، ص81.

³ نهلة قيدوم، مرجع سابق، ص31.

⁴ القانون رقم 10-25، المؤرخ في 24 جويلية 2025، المعدل والمتمم للقانون رقم 01-05 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، ج ر، العدد 48، 2025.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

كما نصت المادة 31 مكرر على توقيع عقوبات جزائية على كل من يخالف أحكام المادة 6 مكرر من قانون رقم 10-25 المعدل والمتمم للقانون رقم 05-01، حيث "يعاقب بالحبس من شهرين (2) إلى سنة (1)، وبغرامة مالية تتراوح من 200.000 دج إلى 1.000.000 دج، أو بإحدى هاتين العقوبتين"¹ من خلال ما تم تناوله سابقا نستنتج أن تبييض الأموال في البيئة الرقمية هو جريمة حديثة تعتمد كلياً على الوسائل الرقمية والتقنيات المتطورة لإخفاء المصدر غير المشروع للأموال، يبتكر المجرمون طرقاً جديدة باستمرار مستغلين "الثورة التكنولوجية" لزيادة أرباحهم والإفلات من العقاب، مما يجعل اكتشاف هذه الجرائم أمراً معقداً، ثم إن جريمة تبييض الأموال في البيئة الرقمية لم تعد تقليدية، بل أصبحت تعتمد على الوسائل الرقمية كركيزة أساسية لها، مما يتطلب تحديثاً مستمراً لأساليب المواجهة ولهذا بذل المشرع الجزائري والمؤسسات الجزائرية جهوداً في الموازنة بين استخدام التكنولوجيا للحماية وبين سن قوانين صارمة لملاحقة مبتكري طرق التبييض الإلكتروني، ولهذا تم بذل جهود دولية للحد منها، وهذا ما سنعالجه في المطلب الثاني.

المطلب الثاني

الجهود الدولية لمكافحة تبييض الأموال في البيئة الرقمية

لقد تم بذل جهود دولية تمثلت في تكريس اتفاقيات وإنشاء هيئات لمكافحة هذه الجرائم ولهذا قسمنا هذا المبحث للاتفاقيات والمنظمات الدولية (الفرع الأول) إضافة إلى المبادرات والآليات متعددة الأطراف التي سعت للحد من هذه الجريمة (الفرع الثاني).

الفرع الأول

الاتفاقيات والمنظمات الدولية

لقد أدرك المجتمع الدولي ضرورة التكاتف لمكافحة جريمة تبييض الأموال في البيئة الرقمية عبر تطوير إطار قانوني ومؤسسي دولي متين، فقد شكلت الاتفاقيات الدولية الركيزة الأساسية التي ألزمت الدول بتجريم غسيل الأموال وتبادل المعلومات، ولضمان تنفيذ الاتفاقيات تم إنشاء منظمات وفرق عمل

¹ القانون رقم 10-25، المؤرخ في 24 جويلية 2025، المعدل والمتمم للقانون رقم 05-01 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، ج ر، العدد 48، 2025.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

متخصصة التي تستهدف منع المجرمين من استغلال النظام المالي، وذلك من خلال إجبار المؤسسات المالية على اتخاذ التدابير العنانية الواجبة لذا سنتناول الاتفاقيات الدولية (أولاً) والمنظمات الدولية (ثانياً).

أولاً. الاتفاقيات الدولية:

تعد اتفاقيات مكافحة جريمة تبييض الأموال في البيئة الرقمية من أهم الصكوك القانونية الدولية التي وضعها المجتمع العالمي لمحاربة ظاهرة تحويل الأموال المتحصلة من جرائم إلى موارد ظاهرها مشروع وسليم.

1- اتفاقية بودابست:

تلعب اتفاقية بودابست لمكافحة الجرائم الإلكترونية دوراً مهماً في إطار مكافحة جرائم تبييض الأموال العابرة للحدود خاصة تلك التي ترتكب عبر وسائل التكنولوجيا الحديثة، ففي ظل التطور الرقمي وانتشار المعاملات المالية عبر الإنترنت والعملات المشفرة، أصبحت آليات التقاضي التقليدية غير كافية لمواجهة عمليات غسل الأموال التي تدار عبر أنظمة حاسوبية وشبكات غير ملومسة.

اتفاقية بودابست هي اتفاقية دولية أقرت في عام 2001 وتعتبر أول معاهدة دولية تتعامل مع جرائم الإنترنت، بهدف لتعزيز التعاون الدولي في مجال مكافحة الجريمة تبييض الأموال وحماية الأمان السيبراني، وهي تحمل اسم العاصمة الهنغارية بودابست التي أُنقِص فيها على نص الاتفاقية¹.

الهدف الرئيسي لاتفاقية بودابست هو تعزيز التعاون الدولي في مكافحة جريمة تبييض الأموال في البيئة الرقمية من خلال تبادل المعلومات والتعاون في التحقيقات وتطوير التشريعات والتدابير اللازمة للحماية السيبرانية من بين النقاط الرئيسية التي تغطيها الاتفاقية:

. تعريف الجرائم الإلكترونية: تعريف مفصل للجرائم الإلكترونية ومجموعة متنوعة من الأنشطة التي تعتبر جرائم إلكترونية ومنها جريمة تبييض الأموال في البيئة الرقمية.

. التحقيق ومتابعة الجرائم: تشجيع الدول على تبادل المعلومات والتعاون في التحقيقات المتعلقة بجريمة تبييض الأموال في البيئة الرقمية وتسهيل متابعة المتهمين عبر الحدود.

. تطوير التشريعات: دعم الدول في تحديث وتطوير التشريعات الوطنية لتجريم الجرائم تبييض الأموال في البيئة الرقمية وتحديد العقوبات اللازمة.

¹ الاتفاقية المتعلقة بالجريمة الإلكترونية، بودابست، مجلس أوروبا، مجموعة المعاهدات الأوروبية، رقم 185، الموقع الرسمي لمجلس

أوروبا <http://www.coe./web/cybercrime/home>

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

. حماية الأمان السيبراني: تعزيز التعاون في مجال الأمان السيبراني واتخاذ التدابير الضرورية لحماية الأنظمة الحيوية والمعلومات الحيوية¹.

. تدريب وبناء القدرات: تقديم التدريب والدعم الفني للدول الأعضاء لتعزيز قدراتها في مجال مكافحة جريمة تبييض الأموال في البيئة الرقمية.

لذا يجب أن تتوافق الدول الأعضاء في اتفاقية بودابست مع مبادئها والتزاماتها وتنفيذها في التشريعات الوطنية والسياسات الوطنية بالإضافة إلى ذلك، يُشجع على تبادل المعلومات والخبرات والبيانات الإحصائية بين الدول الأعضاء للمساهمة في تعزيز الأمان السيبراني ومكافحة الجريمة الإلكترونية على مستوى عالمي.

2-الاتفاقيات الأمم المتحدة:²

تعتبر اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية عام 2000م، مرجعاً لمجموعة من الضوابط والأحكام التي تعمل على الحد من انتشار جريمة تبييض الأموال في البيئة الرقمية عبر الدول والقارات، فقد نصت أحكام المادة 7 من هذه الاتفاقية، على ما يلي:

يتعين على الدول الأطراف أن تنشئ نظاماً داخلياً شاملاً للرقابة والإشراف على المصارف والمؤسسات المالية غير المصرفية وكذلك، حيثما يقتضي الأمر، سائر الهيئات المعرضة بشكل خاص لغسل الأموال في البيئة الرقمية، ضمن نطاق اختصاصها، من أجل ردع كشف جميع أشكال غسل الأموال، ويتعين أن يشدد ذلك النظام على متطلبات تحديد هوية العميل وحفظ السجلات والإبلاغ عن المعاملات المشبوهة من هذه الاتفاقية، وقدرة الأجهزة الإدارية الرقابية، وأجهزة إنفاذ القوانين وسائر الأجهزة المكرسة لمكافحة غسل الأموال (بما فيها السلطات القضائية، حيثما يقضي القانون الداخلي بذلك) أن تكفل دون إخلال بإحكام المادتين (18 و 27) التعاون وتبادل المعلومات على الصعيدين الوطني والدولي ضمن نطاق الشروط التي يفرضها قانونها الداخلي، وأن تنتظر لأجل الغاية في إنشاء وحدة استخبارات مالية تعمل كمركز وطني لجمع وتحليل وتصميم المعلومات عما يحتمل وقوعه من غسل للأموال .

على تلك الدول أن تنتظر في تنفيذ تدابير مجدية للكشف ورصد حركة النقد والصكوك القابلة للتداول ذات الصلة عبر حدودها، رهناً بوجود ضمانات تكفل حسن استخدام المعلومات ودون إعاقة حركة رأس المال المشروع بأي صورة من الصور ويجوز أن تشمل تلك التدابير اشتراط قيام الأفراد والمؤسسات التجارية

¹ الاتفاقية المتعلقة بالجريمة الإلكترونية، رقم 185، مرجع سابق.

² مجموعة العمل المالي لمنطقة الشرق الأوسط وشمال أفريقيا، تقرير التطبيقات حول غسل الأموال عبر الوسائل الإلكترونية، د ط، د د ن، ليبيا، ديسمبر 2017، ص ص 43-44.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

بإبلاغ عن تحويل الكميات الكبيرة من النقد ومن الصكوك القابلة للتداول ذات الصلة عبر الحدود. لدى إنشاء نظام رقابي وإشرافي داخلي بمقتضى أحكام هذه المادة، ودون مساس بأي مادة أخرى من هذه الاتفاقية، يهاب بالدول الأطراف أن تسترشد بالمبادرات ذات الصلة التي اتخذتها المنظمات الإقليمية والمتعددة الأطراف لمكافحة غسل الأموال في البيئة الرقمية.

ب-سعي الدول الأطراف إلى تطوير وتعزيز التعاون العالمي والدولي إقليمي والثنائي بين الأجهزة انفاذ القانون وأجهزة الرقابة المالية من أجل مكافحة غسل الأموال في البيئة الرقمية، وتلزم المادة 18/3 هـ من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية بتقديم السجلات والمستندات والمعلومات التي تقتضيها المساعدة القانونية وذلك بقولها: يجوز أن تطلب المساعدة القانونية المتبادلة، التي تقدم وفقاً لهذه المادة لأي من الأغراض التالية:

- تقديم أصول المستندات والسجلات ذات الصلة، بما فيها السجلات الحكومية أو المصرفية أو المالية أو سجلات الشركات أو الأعمال أو نسخ مصدقة منها، وفرقت المادة (18/29) من الاتفاقية بشأن المساعدة القانونية المتبادلة بين نوعين من المعلومات التي تتضمنها السجلات والوثائق الحكومية:

- المعلومات المتاحة للجميع: أي أنها لا تتسم بالسرية، فلا يجوز للدولة رفض تسليمها، وذلك بقولها: (يتعين على الدولة الطرف متلقيّة الطلب ان توفر للدولة الطرف الطالبة نسخاً من السجلات أو الوثائق أو المعلومات الحكومية الموجودة في حوزتها والتي يسمح قانونها الداخلي بإتاحتها لعامة الناس¹).

- المعلومات ذات الطابع السري: التي لا يجوز للعامة الاطلاع عليها، فيجوز لها وحسب الاتفاقية أن ترفض ولكن بشرط إذا جاء في الفقرة (ب) يجوز للدولة الطرف متلقيّة الطلب حسب تقديرها، أن تقدم إلى الدولة الطرف الطالبة، كلياً أو جزئياً أو رهناً بما تراه مناسباً من شروط، نسخاً من أي سجلات أو وثائق أو معلومات حكومية موجودة في حوزتها ولا يسمح قانونها الداخلي بإتاحتها لعامة الناس.

ثانياً: المنظمات الدولية

لقد ظهرت منظمات دولية تختص بمكافحة هذه الجريمة منها:

¹ مجموعة العمل المالي لمنطقة الشرق الأوسط وشمال أفريقيا، مرجع سابق، ص ص 43-44

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

1. معايير لجنة بازل للرقابة على البنوك:

لجنة بازل للرقابة تم تأسيسها في العام 1974، في مدينة بازل بسويسرا، وتعتبر منظمة دولية لتعزيز التعاون بين البنوك المركزية والوكالات الأخرى سعياً وراء الاستقرار المالي والنقدي، وتقديم خدماتها بشكل حصري للبنوك المركزية والمنظمات الدولية.

أصدرت لجنة بازل عام 1988 بياناً حول منع الاستخدام الإجرامي للنظام المصرفي لأغراض غسل الأموال في البيئة الرقمية المتحصلة من الأنشطة الإجرامية، ولاسيما الاتجار بالمخدرات وبذلك يكون البيان وقرر البيان مجموعة من المبادئ الأساسية لمنع استخدام المصارف في غسل الأموال تضمنت: تحديد هوية العميل، الالتزام بالقوانين، التطابق مع معايير الأخلاقيات العليا والقوانين والأنظمة المحلية، التعاون الكامل مع جهات انفاذ القانون إلى المدى المسموح به دون انتهاك لسرية معلومات العميل، تدريب الموظفين، وحفظ السجلات والتدقيق.

وفي عام 1997م أصدرت لجنة بازل "القواعد الأساسية للرقابة المصرفية الفعالة"، كمرجع أساسي للسلطات المعنية في جميع أنحاء العالم، بهدف أن تتأكد السلطات التنظيمية المشرفة على خدمات المصارف بأن البنوك لديها سياسات، وأساليب، وإجراءات أنظمة دقيقة لمعرفة هوية العميل، والتي تعزز لمعايير أخلاقية ومهنية في القطاع المالي وتمنع أن يستخدم البنك بشكل متعمد وغير متعمد من قبل العناصر الإجرامية، كذلك حثت اللجنة الدول لتبني توصيات مجموعة العمل المالي (FATF)¹

2- توصيات مجموعة العمل الدولية (FATF) وما صدر عنها من أوراق في مجال مكافحة غسل الأموال عبر الوسائل الإلكترونية²:

في عام 1989 قامت مجموعة الدول السبعة في قمته الاقتصادية المنعقدة بمدينة باريس بتشكيل مجموعة العمل المالي (FATF) لمكافحة غسل الأموال في البيئة الرقمية، وبدأت هذه المجموعة المتعددة الجنسيات تعمل بجهد منسق ضد غسل الأموال في البيئة الرقمية على المستوى الدولي. لقد أصبحت توصيات مجموعة العمل المالي المسودة العالمية للضوابط الوطنية والدولية الفعالة المتعلقة بمكافحة غسل الأموال في البيئة الرقمية ومحاربة تمويل الإرهاب، ومن هذه التوصيات:

¹ مجموعة العمل المالي لمنطقة الشرق الأوسط وشمال إفريقيا، مرجع سابق، ص 42.

² المرجع نفسه، ص 44.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

التوصية رقم (15) من التوصيات الأربعين لمجموعة العمل المالي (FATF) بخصوص التقنيات الجديدة، حيث تضمن التوصية بأنه ينبغي على الدول والمؤسسات المالية أن تحدد وتقيم مخاطر غسل الأموال في البيئة الرقمية أو تمويل الإرهاب التي قد تنشأ فيما يتصل بما يلي:

ـ تطوير منتجات وممارسات مهنية جديدة، بما في ذلك الوسائل الجديدة لتقديم الخدمات.

ـ استخدام تقنيات جديدة فيما يتعلق بكل من المنتجات الجديدة والموجودة سابقاً وبالنسبة للمؤسسات المالية. ينبغي أن يتم إجراء تقييم المخاطر هذا قبل إطلاق المنتجات أو الممارسات المهنية الجديدة، أو استخدام التقنيات الجديدة أو التي قيد التطوير، وينبغي عليها أن تتخذ تدابير مناسبة لإدارة تلك المخاطر وخفضها¹. ولم يقتصر دور مجموعة العمل المالي (FATF) على مكافحة صور تبييض الأموال التقليدية، بل امتد ليشمل الجرائم المالية المرتبطة بالبيئة الرقمية، حيث أصدرت توصيات حديثة تتعلق بالأصول الافتراضية ومقدمي خدماتها بهدف تعزيز الرقابة على المعاملات الرقمية والحد من استغلالها في تبييض الأموال في البيئة الرقمية وتمويل الإرهاب²

الفرع الثاني

المبادرات والآليات متعددة الأطراف

لقد كانت الجهود الوطنية الفردية غير كافية لمواجهة هذه الجريمة، ومن هنا برزت المبادرات متعددة الأطراف كضرورة حتمية لتعزيز التعاون الدولي، وتبادل المعلومات وتوحيد الأطر القانونية لملاحقة الجناة ولهذا سنتطرق في هذا الفرع إلى المبادرات متعددة الأطراف (أولاً) قانون باتروت الأمريكي (ثانياً)

أولاً: المبادرات متعددة الأطراف³

اتجه المجتمع الدولي إلى تبني مبادرات متعدد الأطراف تجمع بين دول مختلفة ومنظمات وجهات فاعلة بهدف توحيد الجهود ومكافحة جريمة تبييض الأموال في البيئة الرقمية على الصعيد العالمي.

¹ مجموعة العمل المالي لمنطقة الشرق الأوسط وشمال أفريقيا، مرجع سابق، ص44.

² مجموعة العمل المالي (FATF)، التوصية رقم 15 المتعلقة بالأصول الافتراضية ومقدمي خدماتها، المعدلة سنة 2019.

³ نذير ارتباس، طارق قادري، مرجع سابق، ص405.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

1-منتدى الأمن السيبراني العالمي: يعقد المنتدى اجتماعات دورية لمناقشة التحديات السيبرانية وطرق مواجهتها، وتبادل المعلومات حول التهديدات وأفضل الممارسات، ويضم مشاركين من دول ومنظمات دولية وقطاع الأعمال والأكاديميين والخبراء، كما يعزز التعاون بين الأطراف المعنية لحماية الأمن السيبراني على المستويين الوطني والدولي.¹

2- توجيهات الاتحاد الأوروبي لمكافحة غسل الأموال²:

تعد توجيهات الاتحاد الأوروبي لمكافحة غسل الأموال في البيئة الرقمية (AMLD Anti-Money Launderin Dierctive) الإطار القانوني الموحد الذي يهدف إلى منع استخدام النظام المالي الأوروبي لغسل الأموال في البيئة الرقمية وتمويل الإرهاب، حيث تحدث هذه التوجيهات دورياً لمواكبة التطورات في الجرائم المالية الناشئة.

أصدر الاتحاد الأوروبي تعليمات استشارية في عام 1991، فكانت أول توجيهاته حول منع استخدام النظام المالي لغرض مكافحة غسل الأموال (التوجيه 91/308/الاتحاد الأوروبي) هذا وقد اقتصر أول توجيه صدر على تهريب المخدرات حسب ما هو معرف في معاهدة جنيف لعام 1988، ومع ذلك فإنه تم تشجيع الدول الأعضاء على توسعة ذلك ليشمل الجرائم الأخرى المحتملة، وفي العام 2001 وافق الاتحاد الأوروبي على التوجيه الثاني (توجيه 2001/97/الاتحاد الأوروبي) المعدل للتوجيه السابق، وقد تطلب هذا التوجيه ضوابط أكثر صرامة بخصوص غسل الأموال في البيئة الرقمية في جميع أنحاء القارة، وفي عام 2003 وافقت الدول الأعضاء على تطبيق القانون الوطني، لكن تقيدت بعض الدول بذلك بادئ الأمر وفيما بعد لحقت الدول الأعضاء الأخرى بالمجموعة، وفي عام 2005 اعتمد التوجيه الثالث عن الاتحاد الأوروبي لمنع استخدام النظام المالي لأغراض غسل الأموال وتمويل الإرهاب، استناداً إلى عناصر التوصيات الأربعين المنقحة من مجموعة العمل المالي، وتم الاتفاق على تطبيق التوجيه الثالث في الدول الأعضاء كحد أقصى في 15 ديسمبر 2007 .

ويوجد توجيه سادس الذي دخل حيز التنفيذ في 3 ديسمبر 2020 ولم يتوقف الاتحاد الأوروبي عند التوجيه السادس لمكافحة تبييض الأموال، بل عزز منظومته القانونية سنة 2024 من خلال اعتماد حزمة تشريعية جديدة تضمنت التوجيه رقم 1640/2024 وإنشاء الهيئة الأوروبية لمكافحة تبييض الأموال

¹ المرجع نفسه، ص406.

² مجموعة العمل المالي لمنطقة الشرق الأوسط وشمال إفريقيا، مرجع سابق، ص48.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

(AMLA)، مع توسيع الرقابة لتشمل الأصول الافتراضية ومقدمي خدماتها، بما يعكس توجّهاً حديثاً لمواجهة مخاطر تبييض الأموال في البيئة الرقمية¹.

ثانياً: قانون باتريوت الأمريكي²

ظهر قانون باتريوت الأمريكي بعد هجمات 11 سبتمبر 2001 لتعزيز أدوات مكافحة الإرهاب عبر تقوية القدرات الاستخباراتية والقانونية ويتضمن العنوان الثالث (القانون العام 107-56) إطاراً لمكافحة غسل الأموال وتمويل الإرهاب.

يتناول القانون مسائل النفاذ للبيانات المشفرة عند الحاجة لمكافحة الإرهاب وغسل الأموال، وتشمل التدابير تعزيز إجراءات معرفة العميل والابلاغ عن المعاملات المشبوهة، وتيسير تجميد الأصول الرقمية المرتبطة بكيانات مشبوهة، وتمكين تبادل المعلومات الاستخباراتية والمالية، وفرض متطلبات امتثال تقنية على الجهات المالية ومقدمي خدمات الأصول الرقمية

المبحث الثاني

تحديات الإثبات والملاحقة في جريمة تبييض الأموال في البيئة الرقمية

إنّ جريمة تبييض الأموال في البيئة الرقمية متطورة وهذا انعكس بطبيعة الحال على النظام الإثباتي ولما كان نظام الإثبات في الجزائر هو النظام المختلط وفقاً لنص المادة 212 من قانون الإجراءات الجزائية "أنه يجوز إثبات الجرائم بأي طريق من طرق الإثبات وللقاضي أن يصدر حكمه تبعاً لاقتناعه الشخصي".³ نجد أنّ المشرع منح القاضي الجزائي السلطة التقديرية في تحديد قيمة دليل الإثبات، ومع سكوت المشرع الجزائري عن النص على الأدلة المستمدة من الكمبيوتر كدليل للإثبات فإن القاضي يجد نفسه عاجزاً عن إعمال سلطته التقديرية، والسبب ما يتميز به الدليل الرقمي من خصائص إضافة إلى طرق الإثبات المعمول بها لاستخلاص، ولهذا تدارك المشرع هذا النقص وفقاً لخطته في مكافحة الجريمة التبييض الأموال في البيئة الرقمية بتعديل قانون الإجراءات الجزائية بموجب القانون 06/22 المؤرخ في 27 أبريل 2022، ولمعالجة هذا تطرقنا الى مطلبين ألا وهما: إشكالية الدليل الرقمي وحجته التقنية في إثبات جريمة

¹ Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on anti-money laundering mechanisms

² مجموعة العمل المالي لمنطقة الشرق الأوسط وشمال إفريقيا، مرجع سابق، ص 49.

³ عبير بعقيقي، فيصل نسيغة، الإثبات في الجرائم المعلوماتية على ضوء القانون 09/04، مجلة العلوم القانونية والسياسية، جامعة الوادي، المجلد 9، العدد 02، جوان 2018، ص 35.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

تبييض الأموال في البيئة الرقمية (المطلب الأول) وعوائق الملاحقة القضائية لجريمة تبييض الأموال في البيئة الرقمية (المطلب الثاني)

المطلب الأول

إشكالية الدليل الرقمي وحجته التقنية في إثبات جريمة تبييض الأموال في البيئة الرقمية

إن عملية ضبط الدليل الرقمي والبحث عنه أمر في غاية الصعوبة والتعقيد، إن لم يكن مستحيلاً أحياناً حينما يكون محل البحث هو شبكة الإنترنت بخصوص الجرائم العابرة للحدود، على اعتبار أن التفتيش والضبط في هذه البيئة الافتراضية يتطلب أن يتم خارج حدود الدول، وفي نطاق دولة أخرى. ما يتطلب الحصول على إذن مسبق بذلك من سلطاتها، لما ينطوي عليه من مساس بسيادة هذه الدول، ويعتمد الإثبات على استعمال عدة وسائل تسمى أدلة الإثبات، وبالنسبة للدليل الجنائي فيتمثل في مجموع الوقائع المادية والمعنوية التي تكشف الجريمة تبييض الأموال في البيئة الرقمية.

ويعرف الإثبات الجنائي بأنه كل ما يؤدي إلى معرفة الحقيقة من أجل الحكم على المتهم في المسائل الجنائية بمعنى اثبات وقوع الجريمة ونسبتها للمتهم¹

ولمعالجة هذا سنتطرق في هذا المطلب إلى تعريف الدليل الرقمي وخصائصه (الفرع الأول) وإشكالية قبول الدليل الرقمي في إثبات الجريمة الرقمية وحجته التقنية (الفرع الثاني).

الفرع الأول

تعريف الدليل الرقمي وخصائصه

إن الدليل الرقمي هو عبارة عن معلومات وبيانات مخزنة بصيغة الكترونية عبر الحاسب أو الهواتف الذكية يمكن استخدامها كدليل جنائي أو قانونية وله خصائص وميزات منها أنه غير ملموس وسريع التأثير وسهل النسخ ويحتاج إلى معالجة علمية لاستخلاصه مما يجعله محورياً في قضايا الجرائم المعلوماتية والمعاملات الحديثة سنطرق في هذا الفرع إلى تعريف الدليل الرقمي (أولاً) وخصائصه (ثانياً).

¹ ارتباس نذير، ديابلو محمد نجيب، طارق قادري، الجريمة الالكترونية وحجية الدليل الرقمي في الإثبات الجنائي، ط1، المركز

المغربي شرق أدنى الدراسات الاستراتيجية، المملكة المتحدة البريطانية، جانفي 2024، ص139.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

أولاً: تعريف الدليل الرقمي

عرف الدليل الرقمي بأنه: "الدليل المأخوذ من أجهزة الكمبيوتر في شكل موجات مغناطيسية أو كهربائية يمكن تجميعها وتحليلها بواسطة برامج تطبيقات وتكنولوجيات خاصة"¹ وهناك أيضاً تعريف أكثر شمولاً يعرف الدليل الإلكتروني بأنه: "أي معلومات ذات قيمة إثباتية، يتم تخزينها في شكل رقمي، وتشمل أدلة أجهزة الحاسوب، الفيديو الرقمي، والصوت الرقمي، وأجهزة الفاكس الرقمية، والهواتف المحمولة، والمواقع الإلكترونية"² نستنتج من خلال التعريفات السابقة أن الدليل الرقمي هو كل الوسائل التي تعمل على اكتشاف الجريمة أو اثباتها، والتي تستمد من الواقع الرقمي الافتراضي الذي يعتمد على الأدوات الإلكترونية.

ثانياً: خصائص الدليل الرقمي³

يمتاز الدليل الرقمي بعدة خصائص منها:

- أنه دليل علمي من طبيعة تقنية، فهو يتكون من بيانات ومعلومات ذات هيئة إلكترونية غير ملموسة.
- الحماية من الفقد: هذه الخاصية لا تتوافر في أنواع الأدلة الأخرى، مما يشكل ضماناً شديداً الفعالية للحفاظ على الدليل ضد الفقد والتلف والتغيير.
- صعوبة التخلص منه: الأدلة الرقمية يمكن استرجاعها بعد محوها، وإصلاحها بعد إتلافها، وإظهارها بعد إخفائها، مما يؤدي إلى صعوبة الخلاص منه، وهي ميزة يتمتع بها عن غيره من الأدلة التقليدية، فنشاط الجاني في عملية محو الدليل يشكل في حد ذاته دليلاً ضد الجاني، لأن هذا النشاط يتم تسجيله في الحاسوب الآلي، ويمكن استخلاصه لاحقاً ويترتب على هذه الخاصية مسائل قانونية هامة أبرزها مسألة التخلص أو إخفاء الدليل، وهو يعد فعلاً آخر موضوع تجريم بمقتضى القانون.

¹ نور الهدى محمودي، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية، مجلة الباحث للدراسات الأكاديمية، جامعة باتنة 1، العدد 11، جوان 2017، ص 911.

² بابر صالح محمد المدني، صالح الشريف محمد المدني، حجية الدليل الإلكتروني في إثبات الجريمة المعلوماتية في القانون السوداني (دراسة مقارنة)، المجلة الأكاديمية للبحوث القانونية والسياسية، جامعة عمار ثلجي، الأغواط، المجلد 9، العدد 2، 2025، ص 1051.

³ آمال فكيري، إشكالات الإثبات والاختصاص في جرائم التكنولوجيا الإعلام والاتصال العابرة للحدود، مجلة العلوم القانونية والسياسية، جامعة الشهيد حمة لخضر، الوادي، العدد 17، جانفي 2018، ص 633.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

- إمكانية التوثيق: بالإضافة إلى إمكانية تحديد ما إذا كان الدليل الرقمي قد تم العبث به أو تعديله، وذلك لإمكانية مقارنته بالأصل باستخدام البرامج والتطبيقات الصحيحة.

- الدليل الرقمي هو دليل معنوي غير مرئي سهل الإخفاء ومحي، يشكل عائقاً كبيراً أمام أجهزة العدالة الجنائية لجملة من الأمور، كالتخزين الإلكتروني للمعطيات الذي يجعلها غير مرئية وغير مفهومة بالعين المجردة، وتشفير البيانات المخزنة إلكترونياً أو المنقولة عبر شبكات الاتصال عن بُعد الذي يشكل عقبة كبيرة أمام إثبات جرائم التكنولوجيا الحديثة والبحث عن الأدلة.

الفرع الثاني

إشكالية قبول الدليل الرقمي في إثبات الجريمة الرقمية وحجته التقنية

إن للدليل الرقمي أهمية في إثبات جريمة تبييض الأموال في البيئة الرقمية، لكنه يواجه تحديات مرتبطة بطرق الحصول عليه وإثبات حجته.

لهذا سنعالج في هذا الفرع إلى حجية الدليل الرقمي في إثبات جريمة تبييض الأموال في البيئة الرقمية (أولاً) وشروط قبول الدليل الرقمي كدليل إثبات في الجريمة الرقمية (ثانياً) وسلطة القاضي في قبول الدليل الرقمي (ثالثاً).

أولاً: حجية الدليل الرقمي في إثبات جريمة تبييض الأموال في البيئة الرقمية

يقصد بالحجية: "انها وصف ثابت بحكم الشرع يلحق مضمون الحكم القضائي أو الأمر القضائي فيه ويكون غير قابل للمناقشة فيه مرة أخرى"¹

ومعنى الحجية عند الفقهاء هو "ان القاضي إذا عرضت منازعة امامه في موضوع ما وتنازع الخصوم فيه وفحص القاضي أدلة كل خصم ومستنداته ووزنها ثم قال كلمته الفاصلة في موضوع هذه الدعوى فلا يجوز لأي من الخصوم أن يعيدوا عرض النزاع مرة ثانية لمناقشة ما سبق أن فصل فيه"².

¹ نور الهدى محمودي، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية، مرجع سابق، ص 918.

² المرجع نفسه، ص 918.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

أي يمنع القاضي الذي أصدر الحكم أن يعدل عنه طالما استوفى الحكم شروطه ومتطلباته الشرعية لأن هذا الحكم هو رمز الصواب والصحة وعنوان الحقيقة، وما قيل عن حجية الحكم القضائي يقال كذلك عن حجية الدليل الرقمي.

بمعنى أن حجية الدليل الرقمي هي: "قوته الاستدلالية في إبراز الحقيقة وصدق نسب الفعل الإجرامي إلى شخص معين أو كذبه".¹

يفحص القاضي أدلة كل خصم ومستنداته ووزنها، فلا يجوز لأي من الخصوم أن يبدي عرض النزاع مرة ثانية لمناقشة ما سبق أن فصل في، ويمنع القاضي الذي أصدر الحكم أن يعدل عنه طالما استوفى الحكم شروطه ومتطلباته الشرعية لأن هذا الحكم هو رمز الصواب والصحة وهو عنوان الحقيقة، وما قيل عن حجية الحكم القضائي يقال كذلك عن حجية الدليل الرقمي.²

ثانياً: شروط قبول الدليل الرقمي كدليل إثبات في الجريمة الرقمية

إن الأدلة الرقمية من الأدلة التي تثير إشكالية في قبولها لدى القاضي بسبب عدم تفسيرها مع الحقيقة نظراً لما يمكن أن تخضع له طرق الحصول عليها من التعرض للتزوير والأخطاء المتعددة وسرعة إتلافها أو تغييرها ولم يقيدھا المشرع الجزائري بشروط خاصة بل تركھا للقاضي، لذلك يتعين على القاضي لقبول هذه الأدلة كأسانيد تستند إليها الحقيقة في الدعوى العمومية سواء أكان الحكم فيها بالإدانة أو البراءة توفر بعض الشروط أهمها³:

- أن تكون هذه الأدلة يقينية بحيث تستوجب أن تقترب نحو الحقيقة الواقعية قدر المستطاع وأن تبتعد عن الظنون والتخمينات.

- يتعين مناقشة الدليل الرقمي قضائياً مبدئياً بمرافعة شفوية، فإذا كانت مخرجات الوسائل الرقمية تعد أدلة إثبات قائمة في أوراق الدعوى في الجريمة، فإنها يجب مناقشتها أمام الخصوم .

¹ عبد القادر فلاح، نادية عبد المالك، التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري، مجلة الأستاذ الباحث

للدراسات القانونية والسياسية، جامعة الجيلالي بونعامة، خميس مليانة، المجلد 4، العدد 2، 2019، ص 1701.

² تور الهدى محمودي، مرجع سابق، ص 918

³ المرجع نفسه، ص 919.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

وهنا يتعين على القاضي الاجتهاد في الحكم في جريمة تبييض الأموال في البيئة الرقمية وعدم الاعتماد على رأي الغير إلا إذا كان الغير من الخبراء، فهذا إيراد لخصوص الرأي الفني الذي يستند إليه ضمن حكمه، وبناء عليه يكون متولد من عقيدته وليس من تقرير الخبير.

- يجب أن يكون الدليل الرقمي مشروعاً، ويقصد بذلك أن إجراءات جمع الأدلة الرقمية المستمدة من الحاسب الآلي قد خضعت للقواعد الإجرائية التي تنظم كيفية الحصول عليها، فإنها تكون باطلة ولا تصلح أن تكون أدلة تبنى عليها الإدانة .

ثالثاً: سلطة القاضي في قبول الدليل الرقمي

في الجزائر يسود نظام الإثبات الحر، حيث أن القاضي له الحرية في تكوين عقيدته، غير أنه ملزم بتسبيب حكمه وبيان الأدلة التي استند منها اقتناعه، وبالنظر إلى الأدلة الرقمية المتحصلة من الوسائل الرقمية، فإن قبولها في الإثبات يثير العديد من الإشكالات، ذلك أنه يمكن التلاعب فيها وتغييرها، وبالتالي يجب التحقق من صحتها القاضي يتمتع بحرية تقديرية في قبول هذه الأدلة، فإذا اقتنع بها ووجدتها كافية ومنطقية، يمكنه أن يستند إليها في حكمه¹.

ويتجلى الدور الإيجابي للقاضي الجزائي في الجرائم تبييض الأموال في عنصرين هامين هما:

- توفر الدليل من خلال البحث عن الدليل باستعمال السلطات المخولة له قانوناً، حيث يستطيع: أن يأمر القائم بتشغيل النظام بتقديم المعلومات اللازمة لاختراق النظام والولوج إليه، من خلال الإفصاح عن كلمات المرور والشفرات الخاصة بتشغيل البرنامج

- سلطة الأمر بتفتيش نظم الحاسوب بجميع مكوناته بحثاً عن الدليل الرقم.

وبالتالي تتمثل أهم الضوابط المستمدة من الدليل الرقمي في سلطة القاضي الجزائي في تقديره لهذا الدليل، وهي تستمد من ضرورة الاقتناع بالأدلة الرقمية الصحيحة، وضرورة مناقشته لها في الجلسة مع وجود أصل الدليل في أوراق الدعوى المعروضة في المحكمة²

وبالنظر إلى الطبيعة الخاصة التي تتميز بها الأدلة المتحصلة من الوسائل الرقمية، وما قد يصاحب الحصول عليها من خطوات معقدة، فإن قبولها في الإثبات قد يثير العديد من المشكلات:

¹ نور الهدى محمودي، مرجع سابق، ص 923.

² عبد القادر فلاح، مرجع سابق، ص1702.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

ذلك أنه يمكن التلاعب فيها وتتغير الحقيقة التي يجب أن تعبر عنها، وفي الجزائر فإن الأدلة المتحصلة من الوسائل الرقمية تعد من الأدلة العلمية التي تقبل كطرق إثبات حسب نص المادة 212 من قانون الإجراءات الجزائية، فالمشرع الجزائري لم يضع نصوصاً قانونية صريحة بهذا الخصوص، وإنما تم الاستناد إلى المادة 212 من قانون الإجراءات الجزائية، والتي تقر مبدأ حرية الإثبات.

كما تم إصدار القانون رقم 15/04 سنة 2004 الذي عدل قانون العقوبات وأدخل أحكاماً تتعلق بالجرائم المعلوماتية، ومن بينها تجريم الدخول غير المشروع إلى أنظمة المعالجة الآلية للمعطيات، كما تدخل المشرع الجزائري لاحقاً بحماية المعطيات الرقمية بموجب القانون رقم 04/09 لسنة 2009، الذي ينظم الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال ومكافحتها وقد وضع هذا القانون آليات لضبط الأدلة الرقمية، منها نسخ المعطيات الرقمية، وتحريزها وفق إجراءات قانونية، والاستعانة بالخبراء المختصين¹.

نستنتج من خلال ما سبق أن الدليل الرقمي أصبح عنصراً أساسياً في الكشف عن جريمة تبييض الأموال في البيئة الرقمية وملاحقة مرتكبيها كما أنه يخضع لشروط خاصة في الجمع والحفظ والتحليل لضمان سلامته وحجته القانونية ولذلك كان على المشرع الجزائري استحدث أول قانون إجرائي متعلق بجريمة تبييض الأموال في البيئة الرقمية وهو القانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وقد صدر في وقت مساهم للتطورات التكنولوجية والعلمية.

كما استحدث المشرع الجزائري آليات التحري الخاصة مثل التسرب الإلكتروني، المراقبة الإلكتروني إلا أن هناك العديد من الإشكالات التي تواجه سلطات البحث والتحقيق أهمها القيمة القانونية للأدلة الرقمية ومدى قبولها من طرف القاضي الجزائية حيث يجب أن يكون للدليل الرقمي قيمة قانونية تتعلق بأمرين مهمين هما مشروعية الدليل وحجيته على الوقائع المراد إثباتها، وعلى الرغم من ذلك فإن مجرد تقديم الدليل الرقمي للقاضي يعطيه الصلاحية المطلقة في تقدير هذا الدليل ولا يمكن استبعاده إلا بدليل فني أو إلكتروني آخر.

¹ نور الهدى محمودي، مرجع سابق، ص 923.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

المطلب الثاني

عوائق الملاحقة القضائية لجريمة تبييض الأموال في البيئة الرقمية

يواجه القائمون على عملية محاربة جرائم تبييض الأموال في البيئة الرقمية ببلادنا العديد من العوائق عند إثباتها تحول دون المعالجة الفعالة والحقيقية لظاهرة تبييض الأموال في البيئة الرقمية¹

تقف وسائل الإثبات الجنائي التقليدية عاجزة عن مواجهة هذه الجريمة التي تنصب على المعلومات والبيانات المخزنة في نظم المعلومات والبرامج مما أدى إلى بروز ظاهرة جديدة وهي الظاهرة الرقمية ذات الطبيعة التقنية الناجمة عن الحاسوب والإنترنت نتج عنها ما يسمى الدليل الرقمي لإثبات وقوع الجرائم الإلكترونية ونسبتها لمرتكبيها.

لذا سنتناول في هذا المطلب المعوقات المتعلقة بخصوصية الدليل الرقمي (الفرع الأول) والمعوقات المتعلقة بخصوصية التحقيق (الفرع الثاني).

الفرع الأول

المعوقات المتعلقة بخصوصية الدليل الرقمي

أن هذا الدليل الرقمي تعترضه عدة عقبات في استخلاصه من طرف سلطات التحقيق والتحري وهي عدم ظهور الدليل الرقمي (أولا) وسهولة محوه أو تدميره (ثانيا) وصعوبة الوصول إلى الدليل الرقمي (ثالثا)²:

أولا: عدم ظهور الدليل الرقمي

إن الدليل الرقمي المراد استخلاصه من بيئة رقمية يستمد طبيعته من ذات العمليات الرقمية ولا يمكن كشفه بالطرق التقليدية، وإنما قد يحتاج إلى استخدام تقنيات علمية متطورة يجب إتباعها للوصول إليه، لكونه دليل غير مادي (لموس) وغير مرئي وغير مقروء، بحيث تتجلى هذه الخصوصية من خلال مايلي :

¹دريس باخوية، جريمة تبييض الأموال المكافحة والعوائق، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المركز الجامعي لمتنراست، الجزائر، العدد1، 2012، ص186.

² الطيبي البركة، إشكالية الإثبات في الجرائم الإلكترونية، مجلة الأفاق علمية، المركز الجامعي لمتنراست، المجلد11، العدد1، 2019، ص ص 268-280.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

1-إنها أدلة غير مرئية:

بيانات غير مرئية لا تفصح عن شخصية معينة، وتكون مسجلة رقمياً بكثافة بالغة وبصورة مرمزة لا يمكن للإنسان قراءتها وإن كانت قابلة للقراءة من قبل الأدلة نفسها ولا يترك التعديل أو التلاعب فيها أي أثر مما يقطع أي صلة بين المجرم وجريمته، ويحول دون كشف شخصيته وكشف وتجميع أدلة بهذا الشكل لإثبات وقوع الجريمة ونسبتها إلى مرتكبها هو أحد أهم المشاكل التي يمكن أن تواجه جهات التحري والملاحقة.

2- أن أغلب الآثار المتخلفة عن هذه الجرائم هي آثار رقمية:

هي آثار نبضات رقمية غير مرئية بالعين المجردة فهي تصل في حجمها وشكلها ومكان تواجدها إلى درجة شبه منعدمة، بحيث أنه لا يمكن رؤيتها إلا من خلال الاستعانة بأجهزة ووسائل تقنية تظهرها للعيان، إضافة إلى أن ضخامة حجم وكم البيانات والملفات الرقمية المجرمة من بين ذلك الكم الهائل لفصلها عن تلك البريئة منها وتؤدي في الغالب إلى اصطدام مهمة الاكتشاف بحق الأفراد في الخصوصية الشخصية.

3-أن الجرائم التقليدية يكون فيها الدليل مادي ومرئي ومقروء:

بحيث إن كل الوقائع المتعلقة بهذه الجرائم خاضعة لسيطرة أجهزة العدالة وتخلف آثار مادية كالسكين والسلاح وبقع الدم في جريمة السرقة مثلاً، عكس الجرائم الرقمية التي تكون فيها البيانات والمعلومات عبارة عن نبضات رقمية غير مرئية، والتي غالباً ما تنتفي قدراتهم على أن يتولوا بطريقة مباشرة فحص واختبار البيانات المشتبه فيها وتزداد جسامة هذه المشكلة بوجه خاص في حالة التلاعب في برامج الحاسب نظراً لتطلب الفحص الكامل للبرنامج، و اكتشاف التعليمات غير المشروعة المخفية داخله قدراً كبيراً من الوقت والعمل وغالباً ما لا يكون له من حيث التكلفة الاقتصادية مبرراً¹

4- إن استخلاص الأدلة يعد تحدياً لرجال الأمن:

ذلك أن رجل الأمن غير المتخصص والذي انحصرت معلوماته في جرائم قانون العقوبات بصورة تقليدية من قتل وضرب وسرقة لن يكون قادراً على التعامل مع الجريمة التي تقع بطريقة تقنية عالية ولذلك فغالبية الجرائم تكشف مصادفة وليس بطريق الإبلاغ عنها.

¹الطبيبي البركه، مرجع سابق، ص270.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

كما يرى جانب من الفقه الجنائي أن متطلبات العدالة الجنائية تفرض على الأجهزة الحكومية أن تتحمل كامل مسؤولياتها نحو اكتشاف الجرائم وضبط المجرمين ومحاكمتهم وهذا يتطلب توفير الإمكانيات التقنية اللازمة لتحقيق الجرائم تبييض الأموال وبمعنى آخر يتعين استقطاب وجذب الكفاءات المهنية المتخصصة في هذا المجال للاستعانة بها في تحقيق هذه الجرائم.

وتجدر الإشارة بهذا الخصوص إلى أن المشرع الجزائري تبني وسائل تقنية جديدة لاستخلاص الدليل الرقمي، بموجب المواد 4، 5، 6، 11 من القانون 04-09 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال ومكافحتها، والمتمثلة في مراقبة الاتصالات الإلكترونية، تفتيش المنظومات المعلوماتية، حجز المعطيات المعلوماتية، حفظ المعطيات المتعلقة بحركة السير من طرف مقدمو الخدمات ومنه.¹

ثانياً: سهولة محوه أو تدميره

من المعوقات التي يمكن أن تعترض عمليات الإثبات في جرائم تبييض الأموال في البيئة الرقمية سهولة محوها وتدميرها أدلة الإدانة في فترة زمنية يسيرة.

إلا أننا نشير إلى أن الجاني دائماً ما يحرص على محو الآثار التي تدل على ارتكابه لجريمته من خلال اعتماده على بعض التقنيات التي تساعده على محو وتعديل البيانات الرقمية في أقل مدة ممكنة، كما أن الدليل الرقمي غالباً ما يترك آثاراً في حالة محوه وتعديله، والخبراء المتخصصون فقط من يستطيعون كشف هذه التلاعبات التي يحدثها الجناة في النظم المعلوماتية لمحو آثار جرائمهم.²

ثالثاً: صعوبة الوصول إلى الدليل الرقمي

إن تقديم الأدلة العلمية للمحكمة هي التي تتم عن طريق الشكاوى التي يقدمها المجني ، إلا أن الأمر بالغ التعقيد في الجرائم تبييض الأموال في البيئة الرقمية بالنسبة لجهات التحقيق التي لم تصل إلى تلك المعرفة والخبرة التي تملكها اتجاه التحقيق في الجرائم التقليدية لأن الأمر يتطلب إحاطة كاملة بالتكنولوجيا الحديثة ومعرفة واسعة بالعقبات التي تصعب من الوصول إلى الدليل الرقمي، والمتمثلة فيما يلي:

¹ الطيبي البركة، مرجع سابق، ص 271.

² المرجع نفسه، ص 272.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

1-إحاطته بوسائل الحماية الفنية:

يصعب الوصول إلى الدليل لإحاطته بوسائل الحماية الفنية كاستخدام كلمات السر حول مواقعهم تمنع الوصول إليها أو ترميزها أو تشفيرها لإعاقة المحاولات الرامية إلى الوصول إليها والاطلاع عليها أو استنساخها، وكذا طريق مجموعة من التدابير الأمنية كاستخدام برامج تمنع الوصول إليها أو دس تعليمات خفية بينها أو ترميزها لإعاقة أو منع الاطلاع عليها أو ضبطها.

وهذا ما يعوق رقابة البيانات المخزنة أو المنقولة عبر حدود الدولة والتي تقلل من قدرة جهات التحري والتحقيق والملاحقة على الاطلاع عليها الأمر الذي يجعل حماية حرمة البيانات الشخصية المخزنة في مراكز الحاسبات والشبكات أو المتعلقة بالأسرار التجارية العادية والرقمية أو بتدابير الأمن والدفاع أمر بالغ الصعوبة¹.

2-سلوكات الجاني:

كون الجناة فيها ليسوا أشخاص عاديين بل يتميزون بالذكاء والخبرة الكبيرة في اتقان العمل بالحاسب الآلي وأنظمتهم وبرامجهم، وعليه يتمكنون من إخفاء أفعالهم الإجرامية بسهولة كبيرة، من خلال استخدام التلاعب غير المرئي بما يعرف بالنبضات أو الذبذبات الرقمية التي يتم تسجيل البيانات والمعطيات عن طريقها.

كما أن الإثبات أو الدليل في مثل هكذا قضايا صعب جداً سواء ما تعلق منها بالأدلة المباشرة المتمثلة في اعتراف الجاني، والخبرة ومعاينة مسرح الجرم، الذي يصعب تحديده هو الآخر، أو الأدلة غير المباشرة التي يتحصل عليها القاضي عن طريق الاستقراء والاستنتاج، وإن كان أمر تحصيل الأدلة صعب بالنسبة لهذه الجرائم الواقعة داخل الوطن غير أن تحصيل الأدلة أصعب لما تكون واقعة في الجزائر وآثارها امتدت للخارج²

¹ الطيبي البركة، مرجع سابق، ص273.

² فتحة حمير، الجرائم المعلوماتية في الجزائر: المواجهة والتحدي، مجلة الحقوق والعلوم السياسية، جامعة خنشلة، المجلد12،

العدد1، 2025، ص280.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

3-الامتناع عن التبليغ أو التبليغ بعد فوات الأوان:

إن الأمر ناتج إما عن جهل الضحايا بالقانون، أو عن خوفهم مما قد يترتب عن قيامهم بذلك، فكثير من المؤسسات المالية كالبنوك مثلاً تحجم عن الإبلاغ بحجة أن ذلك سيكون سبباً في تعريض ثقة المتعاملين معها للاهتزاز¹.

كما أن المجني عليه أيضاً يعوق من الوصول إلى الدليل الرقمي بحيث يمتنع في الغالب عن التبليغ عن جريمة تبييض الأموال في البيئة الرقمية وقد يسعى إلى التعتيم على المحققين وتضليلهم حتى لا يكتشفوا هذه الجرائم لهذا لا نعجب إذا وجدنا أن أكثر تلك الجرائم لم تكتشف إلا بمحض الصدفة.

كما أنه بالرغم من حرية القاضي الجنائي في الإثبات إلا أنه لا يستطيع أن يقبل دليلاً متحصل من إجراء غير مشروع، ليس فقط لأن ذلك يتعارض مع قيم العدالة وأخلاقياتها وإنما لأنه كذلك يمس بحق المتهم في الدفاع.²

وقد أثبتت التجارب أن معظم الجهات المجني عليها، لاسيما والتي غالباً ما تكون مصرفاً أو مؤسسة مالية، شركة أو مشروعاً صناعياً ضخماً، قد تمتنع عن الكشف حتى بين موظفيها عما تعرضت لها من اعتداءات رقمية، وذلك بسبب حرص هذه المؤسسات على عدم المساس بسمعتها وفقدان زبائنها والمتعاملين معها الثقة في كفاءتها وقدرتها على حماية مصالحهم، مما قد يترك انطباعاً بعدم اتخاذها للاحتياطات الأمنية اللازمة لحماية معلوماتها، أو لنتيجة إهمالها أو قلة خبرتها أو عدم وعيها الأمني، مما قد ينعكس سلباً على أرباحها وقيمة أسهمها³.

وعليه يمكن القول إن كافة السلوكيات التي يقوم بها المجرم المعلوماتي والمجني عليه أو الضحية في جريمة تبييض الأموال في البيئة الرقمية تصعب من الوصول إلى الدليل الرقمي.

¹ أ فتيحة حمير، الجرائم المعلوماتية في الجزائر: المواجهة والتحدي، مرجع سابق، ص280.

² الطيبي البركة، مرجع سابق، ص275.

³ بوشارب هانية، بن شهرة شلول، معوقات التحقيق الجنائي في البيئة الافتراضية، المجلة الأكاديمية للبحوث القانونية والسياسية،

جامعة غرداية، المجلد7، العدد2، 2023، ص2009.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

الفرع الثاني

المعوقات المتعلقة بخصوصية التحقيق

إن التحقيق في جريمة تبييض الأموال الرقمية أو ما يعرف بالتحقيق الرقمي هو عبارة عن مجموعة من الأساليب المتبعة من أجل معرفة وتقديم معطيات الإعلام مخزنة (الدليل الرقمي) في وسيلة رقمية ممغنطة أمام جهة قضائية

وهذا ما سنعالجه من خلال صعوبة التحري في كشف غموض جريمة تبييض الأموال في البيئة الرقمية (أولاً) وضعف التعاون الدولي في مكافحة جريمة تبييض الأموال في البيئة الرقمية (ثانياً).

أولاً: صعوبة التحري في كشف غموض جريمة تبييض الأموال في البيئة الرقمية

ان التحري في كشف غموض جريمة تبييض الأموال في البيئة الرقمية تعترضها عدة عقبات وتتمثل فيما يلي:¹

1-صعوبة تحصيل الإثباتات والأدلة:

أي تتخلل عملية التحريات والتحقيقات القضائية في القضايا الماسة بأمن المعلومات صعوبات جمة، من أبرزها صعوبة تحصيل المعطيات المتعلقة بمزودي الخدمة لتمرکزها أساساً بالجزائر العاصمة فقط، وعليه فهي تأخذ وقت طویل لتحصيلها.

2-الكم الهائل للبيانات:

يشكل الكم الهائل للبيانات التي يتم تداولها من خلال الأنظمة الرقمية أحد مصادر الصعوبات التي تعوق تحقيق الجرائم التي تقع عليها أو بواسطتها والدليل على ذلك أن طباعة كل ما يوجد على الدعامات الممغنطة لمركز حاسب متوسط الأهمية يتطلب مئات الآلاف من الصفحات، والتي قد لا تثبت كلها تقريباً شيئاً على الإطلاق، مما يصعب من إمكانية تحديد وفصل الجيد ولهذا التحقيق يطول.

¹ فتيحة حمير، مرجع سابق، ص 280.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

3- مميزات جريمة تبييض الأموال الرقمية:

إن جريمة تبييض الأموال في البيئة الرقمية تتميز بحدائثة أساليب ارتكابها وسرعة تنفيذها وسهولة إخفائها ودقة وسرعة محو آثارها وصعوبة التعرف على مرتكبيها وتحتاج لخبرة فنية لكشف المجرم لذلك فقد وجدت صعوبات جمة في كشف غموضها وإجراء التفتيش والضبط اللازمين أو التحقيق فيها على نحو استدعى إعداد برامج تدريب وتأهيل لهذه الموارد من الناحية الفنية على نحو تمكينها من تحقيق المهمة المطلوبة وبكفاءة عالية مما أدى بوقوع الشرطة في أخطاء جسيمة أدت إلى الأضرار بالأدلة الرقمية الخاصة بإثبات الجريمة.¹

4- أساليب التحري التقليدية:

إن أساليب التحري أو التحقيق التقليدية لا تصلح لكشف غموض هذه الجرائم وضبط مرتكبيها والتحفظ على أدلتها، لذلك عمدت العديد من التشريعات إلى وضع أساليب أخرى للتحري عن هذه الجرائم، ومن بينها المشرع الجزائري الذي قام بوضع أساليب تتوافق مع الطبيعة التقنية للتحري عن هذه الجرائم بموجب القانون 09-04 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وأهمها المراقبة الرقمية والتي تحوي أسلوب الوقاية والمكافحة وإجراءات التفتيش في النظم المعلوماتية وحجز الأدلة الرقمية (حجز المعطيات) وحفظ معطيات السير من طرف مقدمي الخدمات، ويبدو أن المشرع الجزائري وبغية تسهيل عمل المحققين في وضع الترتيبات التقنية المشار لها تجاوز كل الحدود ولم يراع حرمة الحياة الخاصة، وقد يكون الدافع إلى ذلك هو طابع الخطورة التي تكتسيه الجريمة إذ أنه ومع سرية المراسلات مضمونة دستورياً وفي المواثيق الدولية كما ورد في المادة 12 من الإعلان العالمي لحقوق الإنسان، وهذه الضمانة الدستورية نص عليها المشرع الجزائري في الفقرة الأولى من المادة 46 من الدستور الحالي، المعدل بموجب القانون رقم 16-01 مؤرخ في 26 جمادى الأولى عام 1437 الموافق 6 مارس 2016، المتضمن التعديل الدستوري.

كما يمكن للمجني عليه في هذه الجرائم أن يقدم خدمات كبيرة لرجال الشرطة أو لسلطة التحقيق بتقديمه معلومات تحقق فائدة كبيرة في معرفة طبيعة الجريمة التي وقعت وأساليب ارتكابها والأدوات المستخدمة في ارتكابها والأشخاص المشتبه فيهم وبواعث الجريمة وما إذا كان هناك شهود أم لا، إضافة

¹ الطيبي البركة، مرجع سابق، ص 275.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

إلى أن إثبات الجرائم التي تقع على العمليات الرقمية باستخدام الوسائل الرقمية سيتأثر بطبيعة هذه الجرائم وبالوسائل العلمية التي قد ترتكب بها، مما قد يؤدي إلى عدم اكتشاف العديد من الجرائم في زمن ارتكابها، أو عدم الوصول إلى الجناة الذين يرتكبون هذه الجرائم، أو تعذر إقامة الدليل اللازم لإثباتها مما يترتب عليه إلحاق الضرر بالأفراد وبالمجتمع¹

نستخلص من كل ما ذكرناه أن التحري في كشف غموض الجريمة من طرف سلطات التحقيق يتطلب تدريبهم وتأهيلهم وإلمامهم بالتقنيات الأساسية لتكنولوجيات الإعلام والاتصال.

ثانياً: ضعف التعاون الدولي في مكافحة جريمة تبييض الأموال في البيئة الرقمية

إن غياب سياسة التعاون الدولي في مقاومة جريمة تبييض الأموال في البيئة الرقمية يعتبر تعاون واضح بين محترفي الإجرام الرقمي فضلاً عن البرامج التي يستعين بها القراصنة في أنشطتهم الإجرامية، مما يزيد فاعلية وخطورة هجومهم وخصوصاً في ظل قصور وعدم فاعلية سياسة الدفاع الخاصة بهذه الجريمة، كما أنه ورغم المناداة بضرورة التعاون الدولي في مكافحة هذه الجريمة إلا أن هناك عوائق تحول دون ذلك وتجعل هذا التعاون صعباً، وأهمها²:

1- عدم وجود نموذج موحد للنشاط الإجرامي:

فالأنظمة القانونية القائمة في الكثير من الدول لمواجهة الجرائم تبييض الأموال في البيئة الرقمية لا يوجد فيها اتفاق عام مشترك حول نماذج إساءة استخدام نظم المعلومات وشبكة الإنترنت الواجب تجريمها، فما يكون مباحاً في بعض الأنظمة يكون محرماً في أنظمة أخرى، ويرجع ذلك إلى عدة عوامل كاختلاف العادات والتقاليد والديانات والثقافات من مجتمع لآخر.

2- اختلاف النظم القانونية الإجرائية:

بسبب تنوع واختلاف النظم القانونية الإجرائية نجد أن طرق التحري والتحقيق والمحاكمة التي تثبت فائدتها وفعاليتها في دولة ما قد تكون عديمة الفائدة في دولة أخرى، عدم وجود معاهدات ثنائية أو جماعية

¹ الطيبي البركة، مرجع سابق، ص 278.

² المرجع نفسه، ص 279.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

بين الدول: وحتى في حالة وجودها فإنها تكون قاصرة عن تحقيق الحماية المطلوبة في ظل التقدم السريع لنظم وبرامج الحاسب وشبكة الإنترنت¹.

3- مشكلة الاختصاص في جرائم الإنترنت:

إن نقص الخبرة الفنية والتقنية والمعرفة اللازمة بالحاسب الآلي وأنظمتها لدى العديد من المكلفين بعملية مكافحة هذه الجرائم تثير مشكلة بالنسبة للاختصاص على المستوى الدولي وذلك لاختلاف التشريعات والنظم القانونية من دولة لأخرى، حيث ينجم عنها تنازع الاختصاص بين هذه الدول بالنسبة للجرائم المتعلقة بالبيئة الرقمية التي تتميز بكونها عابرة للحدود، فيحدث أن ترتكب داخل إقليم دولة معينة إلا أنها تمتد إلى خارج إقليم دول أخرى مما يعني خضوعها لأكثر من قانون جنائي².

4- عدم وجود قنوات اتصال:

أن من أهم الأهداف المرجوة من التعاون الدولي في مجال الجريمة والمجرمين هي الحصول على المعلومات والبيانات المتعلقة بهم ولتحقيق هذا الهدف كان لازماً أن يكون هناك نظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أمنية لجمع الأدلة، فعدم وجود مثل هذا النظام يعني عدم القدرة على جمع الأدلة التي غالباً ما تكون مفيدة في التحري لجرائم معينة ولمجرمين معينين وبالتالي تنعدم الفائدة من هذا التعاون

لذا أصبح أمر التعاون الدولي لمكافحة جريمة تبييض الأموال في البيئة الرقمية أمراً حتمياً يستلزم ضرورة إيجاد الوسائل المناسبة لتشجيع التعاون لمواجهة هذه الجريمة، والعمل على التوفيق بين التشريعات الخاصة التي تتناول هذه الجريمة، ويجب أن يشمل هذا التعاون تبادل المعلومات، تسليم المجرمين، سبل المكافحة، وضمان أن الأدلة التي يتم جمعها في دولة تقبل في محاكم دول أخرى، وتعد الوسيلة المثلى للتعاون الدولي في هذا الخصوص هو إبرام الاتفاقات الدولية، وفي مجال الإجراءات فإن التوافق بين مختلف سلطات التدخل الوطنية سيكون هاماً من أجل التمييز دون عقبة لطلب المساعدة القانونية الوطنية، ويسهل

¹ الطيبي البركة، مرجع سابق، ص 279.

² المرجع نفسه، ص 280.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

من عملية القبض على مرتكبي هذه الجريمة، وذلك دون مساس هذه الإجراءات بسيادة الدول الأخرى وأمنها ونظامها العام أو أي مصلحة أخرى من مصالحها الأساسية¹.

كما تجدر الإشارة إلى أن المشرع الجزائري نص في الفصل السادس من القانون 09-04 المؤرخ في 5 أوت 2009، السالف الذكر، على قواعد تتعلق بالاختصاص القضائي والمساعدة القضائية الدولية المتبادلة وتبادل المعلومات واتخاذ الإجراءات التحفظية ووضع قيود على طلبات المساعدة القضائية الدولية التي من شأنها المساس بالسيادة الوطنية أو النظام العام.

نستنتج من خلال ما سبق أن مسألة الإثبات تثير صعوبات في مواجهة جرائم تبييض الأموال في البيئة الرقمية، بسبب أن هذه الجرائم تقنية تنشأ في الخفاء ببيئة رقمية، يقتربها مجرمون أذكيا يمتلكون أدوات المعرفة التقنية للنيل من الحق في المعلومات، ينتج عنها ما يعرف بالأدلة الرقمية التي تعتبر إحدى الآثار المهمة في الكشف عن هذه الجريمة والربط بينها وبين مرتكبيها، وأن الدليل الرقمي عند استخلاصه تعترضه عدة عقبات منها ما يتعلق بخصوصية الدليل الرقمي في حد ذاته بسبب عدم ظهوره وسهولة محوه أو تدميره وصعوبة الوصول إليه، ومنها ما يتعلق بخصوصية التحقيق بسبب صعوبة التحري في كشف غموض الجريمة وضعف التعاون الدولي في مكافحة جريمة تبييض الأموال في البيئة الرقمية، كما أنه لتسهيل عملية جمع الأدلة الرقمية تم تحديث الأساليب الإجرائية لمواجهة وقوع هذه الجريمة من طرف المشرع الجزائري وبعض الدول.

¹ الطيبي البركة، مرجع سابق، ص 280.

الفصل الثاني: آليات مكافحة جريمة تبييض الأموال في البيئة الرقمية وإشكالات الملاحقة.

خلاصة الفصل الثاني

وفي الأخير يمكن القول إنه بالرغم من التحديات المستمرة في مواجهة جريمة تبييض الأموال في البيئة الرقمية التي تتطور باستمرار مع تطور التكنولوجيا، إلا أن الجهود المشتركة الوطنية والدولية والتفاني في مكافحة هذه الجريمة يمثل خطوة كبيرة نحو تحقيق بيئة معلوماتية أكثر أماناً وموثوقية، وللمساهمة في الوقاية وكذا التصدي لجرائم تبييض الأموال في البيئة الرقمية.

ورغم تضافر هذه الجهود الوطنية والدولية في مكافحة جريمة تبييض الاموال في البيئة الرقمية تظل عملية الإثبات والملاحقة تواجه عقبات قانونية وتقنية معقدة، فإثبات جريمة في التشريع الجزائري يواجه العديد من الصعوبات والإشكاليات التي تعرقل وتمنع من التوسع في مجال كشف وضبط هذه الجرائم بسبب أن هذه الجرائم تقنية تنشأ في الخفاء ببيئة إلكترونية، يقترفها مجرمون أذكاء يمتلكون أدوات المعرفة التقنية للنيل من الحق في المعلومات، ينتج عنها ما يعرف بالأدلة الرقمية التي تعتبر إحدى الآثار المهمة في الكشف عن هذه الجريمة والربط بينها وبين مرتكبيها، كما أن الدليل الرقمي عند استخلاصه تعترضه عدة عقبات منها ما يتعلق بخصوصية الدليل الإلكتروني في حد ذاته بسبب عدم ظهوره وسهولة محوه أو تدميره وصعوبة الوصول إليه، ومنها ما يتعلق بخصوصية التحقيق بسبب صعوبة التحري في كشف غموض الجريمة وضعف التعاون الدولي في مكافحة الجرائم الإلكترونية.

الخاتمة

الخاتمة

الخاتمة

تعتبر جريمة تبييض الأموال في البيئة الرقمية من أخطر الجرائم الاقتصادية الحديثة، فهي تتميز باعتمادها على الوسائل التكنولوجية الحديثة والتقنيات الرقمية المتطورة لإخفاء المصدر الأموال غير المشروعة وتمويه حقيقتها، بما يتيح للجناة الإفلات من العقاب، وقد ساهم التطور التكنولوجي وظهور وسائل الدفع الإلكترونية والعملات الرقمية في سهولة ارتكاب هذه الجريمة وتوسيع نطاقها على المستويين الوطني والدولي.

كما تبين أن جريمة تبييض الأموال في البيئة الرقمية لا تختلف من حيث الهدف عن الجريمة التقليدية، إذ تسعى كلاهما إلى إضفاء الصفة المشروعة على الأموال غير المشروعة، غير أن الاختلاف يكمن أساساً في الوسائل والآليات والأساليب المستخدمة في ارتكابها، والتي أصبحت أكثر تعقيداً وخفاءً في البيئة الرقمية.

ونظراً لخطورة هذه الجريمة وانعكاساتها السلبية على الفرد والمجتمع، فقد عملت مختلف الدول، ومنها الجزائر، على وضع آليات قانونية ومؤسسية لمكافحةها، سواء من خلال سن تشريعات وطنية أو عبر الاتفاقيات الدولية تهدف إلى الوقاية منها والتصدي لمرتكبيها غير أن الدراسة أظهرت وجود قصور تشريعي في مواكبة التطورات التقنية المتسارعة، إذ ما تزال بعض النصوص القانونية تركز على الصور التقليدية لجريمة تبييض الأموال، دون الإحاطة الكاملة بالصور الرقمية المستحدثة وأساليب ارتكابها الحديثة.

ومن خلال تحليلنا ودراستنا لإشكالية البحث، اتضح أن البيئة الرقمية ساهمت بشكل كبير في تطور جريمة تبييض الأموال وتعقيد أساليب ارتكابها، نتيجة الاعتماد على الوسائل التكنولوجية الحديثة والعملات الرقمية الأمر الذي جعل آليات المكافحة التقليدية غير كافية لمواجهتها، كما تبين أن التشريع الجزائري، رغم الجهود المبذولة، لا يزال بحاجة إلى تطوير وتحديث لمواكبة التحولات الرقمية المتسارعة وتحقيق فعالية أكبر في مجال الوقاية والكشف والمتابعة.

ومن خلال هذه الدراسة تم التوصل إلى مجموعة من النتائج أهمها:

- احتفاظ المشرع الجزائري بنفس التكييف القانوني المطبق على جريمة تبييض الأموال التقليدية رغم خصوصية البيئة الرقمية.

الخاتمة

- أن جريمة تبييض الأموال في البيئة الرقمية تتميز بطبيعة خاصة، نظراً لارتباطها بفضاء افتراضي يصعب تعقب معاملاته وإثباتها.
- اعتماد المشرع لنفس الجزاءات المقررة للجريمة التقليدية دون تخصيص نصوص جزائية تتلاءم مع خصوصية الجريمة الرقمية.
- تمثل العملات المشفرة أحد أهم أبرز الوسائل الحديثة المستعملة في عمليات تبييض الأموال الرقمية.
- تمر جريمة تبييض الأموال بعدة مراحل أساسية تتمثل في التوظيف، والتجميع، ثم الدمج بهدف إضفاء الشرعية على الأموال غير المشروعة.
- تثير عملية إثبات جريمة تبييض الأموال الرقمية عدة صعوبات، خاصة فيما يتعلق بالدليل الرقمي وإجراءات التحري والتحقيق.

الإقتراحات

- وبناءً على ما سبق، يمكن اقتراح مايلي:
- يجب تحديث المنظومة التشريعية الجزائية بما يواكب التطورات الرقمية الحديثة.
- ضرورة سن قانون مستقل خاص بالجرائم الرقمية وإقرار المزيد من الجزاءات العقابية الرادعة على هذا النوع المستحدث من السلوكيات الإجرامية.
- ضرورة تعزيز التعاون الدولي وتبادل المعلومات والتجارب لمكافحة جريمة تبييض الاموال في البيئة الرقمية.
- تطوير المنظومة التشريعية في مجال الإثبات الرقمي وتدعيم آليات التحقيق الالكتروني.
- تأهيل الجهات الأمنية والقضائية تقنياً من خلال التكوين والتدريب المتخصص.
- يجب تشجيع التوعية بأمان الإنترنت بمخاطر الجرائم الرقمية وسبل الوقاية منها ويمكن تحقيق ذلك من خلال الحملات التوعوية وورش العمل والموارد التعليمية .
- نشر الوعي المجتمعي.

الخاتمة

- تشجيع الكفاءات المحلية، على تطوير أنظمة حماية معلوماتية فعالة قصد تأمين مجالنا المعلوماتي والقومي.

وفي الأخير يمكننا القول إن مكافحة جريمة تبييض الأموال في البيئة الرقمية رهينة بمدى فعالية التشريعات الوطنية والتعاون الدولي، إلى جانب مواكبة التطور التكنولوجي المستمر، بما يضمن حماية الاقتصاد الوطني وتعزيز الأمن المعلوماتي والمالي.

قائمة المصادر والمراجع

قائمة المصادر والمراجع:

أولاً: المصادر

1 - الاتفاقيات والمعاهدات الدولية:

- الاتفاقية المتعلقة بالجريمة الالكترونية، بودابست، مجلس أوروبا، مجموعة المعاهدات الأوروبية، رقم 185، الموقع الرسمي لمجلس أوروبا.
- مجموعة العمل المالي (FATF)، التوصية رقم 15 المتعلقة بالأصول الافتراضية ومقدمي خدماتها، المعدلة سنة 2019.

2- القوانين والأوامر:

- الأمر رقم 66. 156 المؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات، الجريدة الرسمية، العدد 49، 1966.
- الأمر رقم 22/96 المؤرخ في 09/07/1996، المتعلق بقمع مخالفة التشريع والتنظيم الخاصين بالصرف وحركة رؤوس الأموال من وإلى الخارج، الجريدة الرسمية، العدد 43، 1996.
- القانون رقم 01-05 المؤرخ في 2005/2/6، المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب مكافحتها، الجريدة الرسمية، العدد 11، 2005.
- القانون رقم 06-05 المؤرخ في 23 أوت 2005، المتعلق بمكافحة التهريب، الجريدة الرسمية، العدد 59، 2005.
- القانون رقم 01-06 المؤرخ في 20 فبراير 2006، المتعلق بالوقاية من الفساد ومكافحته، الجريدة الرسمية، العدد 14، 2006.
- القانون 01-09 المؤرخ في 25 فبراير 2009 المعدل والمتمم للأمر 66-156 المؤرخ 8 يونيو 1966، المتضمن قانون العقوبات الجريدة الرسمية، العدد 15، 2009
- القانون رقم 04-09 المؤرخ بتاريخ 5 أوت 2009، المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، 2009.
- الأمر رقم 02-12 المؤرخ 2012/2/13، يعدل ويتم القانون رقم 01-05 المؤرخ في 2005/2/6، المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب، ومكافحتها، الجريدة الرسمية، العدد 8، 2012.
- القانون رقم 05-18 المؤرخ في 10 ماي 2018، المتعلق بالتجارة الإلكترونية، الجريدة الرسمية، العدد 28، 2018.

- القانون رقم 22-8 المؤرخ في 5 ماي 2022، المعدل والمتمم لقانون 06-01 المؤرخ 20 فيفري 2006، المتعلق بالوقاية من الفساد ومكافحته، الجريدة الرسمية، العدد 32، 2022.
- القانون رقم 154 لسنة 2022، الصادرة بتاريخ 15 يونيو 2022، جمهورية مصر العربية، المعدل لقانون رقم 80، 2002 بشأن مكافحة غسل الأموال، الجريدة الرسمية، العدد 23 مكرر.
- القانون رقم 10.25 المؤرخ في 24 جويلية 2025 المعدل للقانون 01-05 المؤرخ في 27 ذي الحجة عام 1425 هـ الموافق لـ 06 فبراير 2005 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحته، الجريدة الرسمية، العدد 48.

3- المراسيم:

- المرسوم الرئاسي 08-44، المؤرخ في فبراير 2008، المتضمن إنشاء مركز الوقاية من الجرائم الإعلام الآلي والاتصال وتحديد مهامه وتنظيمه، الجريدة الرسمية، العدد 8، 2008.
- المرسوم التنفيذي، رقم 22.36 المؤرخ في 4 جانفي 2022، المتضمن إنشاء خلية معالجة الاستعلام المالي وتنظيمها وسيرها المادة 04، المتضمن إنشاء خلية معالجة الاستعلام المالي وتنظيمها وعملها، الجريدة الرسمية، العدد 3، 2022.

4- الأنظمة:

- النظام رقم 12-03 المؤرخ في 28/11/2012، المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، الجريدة الرسمية، العدد 12، 2013.
- النظام رقم 25-14 المؤرخ في 24 سبتمبر 2025، يعدل ويتم النظام رقم 24-03 المؤرخ في 24 يوليو 2024، المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب وتمويل انتشار أسلحة الدمار الشامل ومكافحتها، الجريدة الرسمية، العدد 68، 2025.

ثانيا: المراجع

الكتب باللغة العربية:

1- الموسوعات:

- أحمد إبراهيم دهشان، يحي إبراهيم دهشان، موسوعة الجرائم الاقتصادية أساليب غسل الأموال التقليدية والحديثة مراحل وآليات الجريمة، الشروط الأساسية للجريمة، أركان الجريمة، جزء 2، دون طبعة، الدهشان للمحاماة والاستشارات القانوني، 2025.

2-الكتب القانونية:

- نادر عبد العزيز شافي، تبييض الأموال دراسة مقارنة، منشورات حلبي الحقوقية، 2001.
- إبراهيم بختي، التجارة الإلكترونية: مفاهيم وإستراتيجيات التطبيق في المؤسسة، طبعة 1، ديوان المطبوعات الجامعية، الجزائر، 2005.
- أحسن بوسقيعة، الوجيز في القانون الجزائري الخاص، جزء 2، طبعة 10، دار الهومة، الجزائر، 2008.
- ارتباس نذير، ديابلو محمد نجيب، طارق قادري، الجريمة الالكترونية وحجية الدليل الرقمي في الإثبات الجنائي، ط1، المركز المغربي شرق أدنى الدراسات الاستراتيجية، المملكة المتحدة البريطانية، جانفي 2024.
- أمجد سعود القطيفان الخريشة، جريمة غسل الأموال دراسة مقارنة، طبعة 1، دار الثقافة للنشر والتوزيع، الأردن، 2006.
- دليلة جلالية، جريمة تبييض الأموال، ط1، دار المثقف العربي، الجزائر، 2025.
- علي العريان، عمليات غسل الأموال وآليات مكافحتها، دون طبعة، دار الجامعية الجديدة للنشر، الإسكندرية، مصر، 2009.
- مجموعة العمل المالي لمنطقة الشرق الأوسط وشمال افريقيا، تقرير التطبيقات حول غسل الأموال عبر الوسائل الالكترونية، دون طبعة، دن، ليبيا، ديسمبر 2017.
- محمود محمود مصطفى، الجرائم الاقتصادية في القانون المقارن، ج1، ط1، مطبعة القاهرة والكتاب الجامعي، مصر، 1979.

3-أطروحات الدكتوراه:

- حميد قطوش، دراسة فعالية منظومة محاربة تبييض الأموال وتمويل الإرهاب في الجزائر، أطروحة مقدمة لنيل شهادة الدكتوراه في علوم التسيير، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة الجزائر 3، 2018/2019.
- فريد علواش، جريمة غسيل الأموال دراسة مقارنة، أطروحة الدكتوراه العلوم في الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2008-2009.

4-مذكرات الماجستير:

- محمد خميخم، الطبيعة الخاصة للجريمة الاقتصادية في التشريع الجزائري، مذكرة لنيل شهادة الماجستير في القانون الجنائي والعلوم الجنائية، كلية الحقوق بن عكنون، جامعة الجزائر، 2010-2011.

5- مذكرات الماستر:

- سرارية عيشوش، جريمة تبييض الأموال وفق التشريع الجزائري، مذكرة مكملة من متطلبات شهادة الماستر في الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2016/2015.
- نهلة قيدوم، بريق وصال درة القدس، جريمة تبييض الأموال باستخدام الوسائط الإلكترونية، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة محمد الشريف مساعدي، سوق اهراس، 2023.

6- المقالات العلمية:

- صالح شنين، التسرب في قانون الإجراءات الجنائية الجزائري حماية للنظام العام والحريات أم حماية للنظام العام، المجلة الجزائرية للقانون المقارن، جامعة أبو بكر بلقايد، تلمسان، العدد2، 2015.
- فتيحة بنابي، العملات المشفرة كوجه حديث للعملات الرقمية، تطبيقاتها وأثارها على المعاملات البنكية-بنك سيليكون فاليس نموذجاً-، مجلة اقتصاديات الأعمال والتجارة، جامعة محمد بوضياف المسيلة، العدد01، مارس2024.
- الطيبي البركة، إشكالية الإثبات في الجرائم الإلكترونية، مجلة الأفاق علمية، المركز الجامعي لتمنراست، المجلد11، العدد1، 2019.
- المختار بن قوية، جريمة تبييض الأموال بين الأساليب التقليدية والتكنولوجيات الحديثة، المجلة المتوسطية للقانون والاقتصاد، جامعة أكلي محند أولحاج، البويرة، المجلد9، العدد1، 2024.
- عادل عكروم، جريمة تبييض الأموال دراسة مقارنة، جامعة سعد دحلب، دون عدد، دون تاريخ نشر.
- عبد الرحمان خلفي، المسؤولية الجنائية للأشخاص المعنوية في جرائم تبييض الأموال، المجلة الأكاديمية للبحث القانوني، جامعة عبد الحمان ميرة، بجاية، العدد2، 2011.
- عبد الرؤوف دباش، هشام ذبيح، وسائل الدفع مابين الحماية التقنية والقانونية للمستهلك الإلكتروني، مخبر أثر الاجتهاد القضائي على حركة التشريع، جامعة محمد خيضر، بسكرة، العدد14، 2014.

- عبد القادر فلاح، نادية آيت عبد المالك، التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، المسيلة، العدد2، 2019.
- عبد القادر فلاح، نادية عبد المالك، التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة الجيلالي بونعامة، خميس مليانة، المجلد4، العدد2، 2019.
- عبير بعقيقي، فيصل نسيغة، الإثبات في الجرائم المعلوماتية على ضوء القانون 09/04، مجلة العلوم القانونية والسياسية، جامعة الوادي، المجلد9، العدد02، جوان 2018.
- عثمان خرشي، الترصد الإلكتروني كآلية لمكافحة الجرائم المعلوماتية، مجلة الدراسات الحقوقية، جامعة الطاهر مولاي، سعيدة، العدد3، 2020.
- عز الدين بوبكر مصطفى شرون، العملات المشفرة مستقبل المعاملات المالية -البنكوك نموذجاً-، مجلة المنهل الإقتصادي، جامعة الوادي، العدد4، ديسمبر 2019.
- فتحة حمير، الجرائم المعلوماتية في الجزائر: المواجهة والتحدي، مجلة الحقوق والعلوم السياسية، جامعة خنشلة، المجلد12، العدد1، 2025.
- فتحة يوسف، هداية بوعزة، الحماية التقنية للمعلومات ودورها في تأمين نظام الدفع الإلكتروني، مجلة الدراسات والبحوث القانونية، جامعة محمد بوضياف، المسيلة، العدد4، 2018.
- فريد ناشف، جريمة تبييض الأموال من منظور التشريع الجزائري، مجلة الحقوق والحريات، جامعة البليدة02، المجلد10، العدد01، 2022.
- كمال مهدي، دريس باخويا، دور الوسائط التكنولوجية في انتشار جرائم تبييض الأموال وآليات مكافحتها، المجلة الإفريقية للدراسات القانونية والسياسية، جامعة أدرار، العدد2، ديسمبر 2018.
- محمد شايب، نعيمة برك، الوقاية من تزوير بطاقات الدفع الإلكترونية كآلية للحد من الفساد المالي في البنوك والمؤسسات المالية، مجلة دفاقر اقتصادية، جامعة زيان عاشور، الجلفة، العدد1، 2011.
- مهدي رضا، الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري، مجلة ايليزا للبحوث والدراسات، جامعة زيان عاشور، الجلفة، المجلد06، العدد02، 2021.

- ناجي بولمناخر، البحث العلمي في ظل البيئة الرقمية: تحديات الواقع وأفاق المستقبل، مجلة دفاتر المتوسط، جامعة باجي مختار، عنابة، المجلد 6، العدد 2، ديسمبر 2021.
- ناجية شيخ، أساليب البحث والتحري المستحدثة في القانون رقم 06.22 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري، المجلة النقدية، جامعة مولود معمري، تيزي وزو، العدد 1، 2013.
- نجا فتور، عادل شيهب، البيئة الرقمية للتعليم عن بعد في الجامعة الجزائرية قراءة في التحديات والانعكاسات من وجهة نظر الأساتذة والطلبة في جامعة جيجل، مجلة دراسات اقتصادية، الجلفة، جامعة زيان عاشور، المجلد 17، العدد 3، 2023.
- نصر الشريف العربي، أساليب التحري في جرائم الفساد، دراسات الوظيفة العامة، المركز الجامعي نور البشير، البيض، العدد 4، 2017.
- نور الهدى محمودي، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية، مجلة الباحث للدراسات الأكاديمية، جامعة باتنة 1، العدد 11، جوان 2017.
- هدى زوزو، التسرب كأسلوب من أساليب التحري في القانون الإجراءات الجزائية الجزائري، مجلة دفاتر السياسية والقانون، جامعة قاصدي مرباح، ورقلة، العدد 11، 2014.
- وديع أسامة وجدي، خصائص العملات المشفرة بين المنافع والتهديدات التنظيمية، المجلة العلمية للاقتصاد والتجارة، جامعة عين شمس مصر، العدد 4، نوفمبر 2019.
- يزيد بوحليط، السياسة الجنائية في مجال تبييض الأموال في الجزائر، دون طبعة، دار الجامعة الجديدة، الجزائر، 2014.
- ارتباس نذير، طارق قادري، الجريمة الالكترونية وحجية الدليل الرقمي في الاثبات الجنائي، المركز المغاربي، ط 1، جانفي 2024.
- آمال فكيري، إشكالات الإثبات والاختصاص في جرائم التكنولوجيا الإعلام والاتصال العابرة للحدود، مجلة العلوم القانونية والسياسية، جامعة الشهيد حمة لخضر، الوادي، العدد 17، جانفي 2018.
- آمنة تازير، جريمة تبييض الأموال في التشريع الجزائري بين القمع والوقاية، مجلة دراسات إنسانية واجتماعية، جامعة وهران 3، العدد 10، جوان 2019.

- أيمن بوزانة، وفاء حمدوش، التجارة الإلكترونية في سياق القانون رقم 05-18 والمراسيم التنفيذية المتعلقة بالسجل التجاري الإلكتروني في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة عنابة، العدد 01، جوان 2021.
- بابكر صالح محمد المدني، صالح الشريف محمد المدني، حجية الدليل الإلكتروني في إثبات الجريمة المعلوماتية في القانون السوداني (دراسة مقارنة)، المجلة الأكاديمية للبحوث القانونية والسياسية، جامعة عمار ثليجي، الأغواط، المجلد 9، العدد 2، 2025.
- بوشارب هانية، بن شهرة شلول، معوقات التحقيق الجنائي في البيئة الافتراضية، المجلة الأكاديمية للبحوث القانونية والسياسية، جامعة غرداية، المجلد 7، العدد 2، 2023.
- جمال براهيم، مكافحة الجريمة الإلكترونية في التشريع الجزائري، المجلة النقدية للقانون والعلوم السياسية، جامعة مولود معمري، تيزي وزو، العدد 02، 2016.
- حسام منصور، الإشهار في البيئة الرقمية مفاهيم أساسية، مجلة التمكين الاجتماعي، جامعة عمار ثليجي، الأغواط، المجلد 4، العدد 02، جوان 2022.
- خالد بغداد، التنظيم القانوني للعمليات المشفرة، (مذكرة ماستر) كلية الحقوق، المركز الجامعي مغنية، 2019.
- خديجة خلوفي، فريدة لوني، أركان جريمة تبييض الأموال في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف المسيلة، المجلد 2، العدد 8، 2017.
- دريس باخويا، أحكام مكافحة جريمة تبييض الأموال في التشريع الجزائري، مجلة جامعة أدرار، العدد 6، جوان 2016.
- دريس باخوية، جريمة تبييض الأموال المكافحة والعوائق، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المركز الجامعي لمتنراست، الجزائر، العدد 1، 2012.
- ذهبية لعجال، الأساليب الحديثة لتبييض الأموال في ظل التطور التكنولوجي، مجلة الاجتهاد القضائي، جامعة بسكرة، العدد 25، جانفي 2021.
- زiegam أبو القاسم، الآليات الدولية والوطنية لمكافحة جريمة تبييض الأموال، مجلة القانون الدولي والتنمية، جامعة عبد الحميد ابن باديس، مستغانم، العدد 5، 2016.

- سعاد رابح، ضوابط مكافحة الجريمة المعلوماتية، مجلة القانون العام الجزائري والمقارن، جامعة الجيلالي الياصب، سيدي بلعباس، العدد1، 2021.
- سعيد فروحات، الوقائية والقمعية لمكافحة تبييض الأموال في الجزائر، مجلة الواحات للبحوث والدراسات، جامعة غرداية، العدد1، 2015.
- سعيدة بوزنون، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة العلوم الإنسانية، جامعة محمد خيضر، بسكرة، العدد3، 2019.
- فاضلي سيد علي، التنظيم القانوني للجريمة الاقتصادية وخصوصيتها في التشريع الجزائري، مجلة دفاتر اقتصادية، جامعة المسيلة، الجزائر، المجلد 14، العدد1، 2023.
- لوني فريدة، القواعد العامة للجرائم الاقتصادية في التشريع الجزائري، مجلة الدراسات الحقوقية، جامعة أكلى محند اولحاج البويرة، الجزائر، المجلد9، العدد2، ديسمبر2022.

المراجع باللغة الأجنبية:

1-European parliament regulation:

-Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on anti-money laundering mechanisms.

2-dictionnaires:

- Le nouveau petit robert dictionnaire alphabetique et analogique de la languefrançaise(relie)de Josette Rey ,Debove,Auteur,2005.
- Petit Larousse illustre coffret noiel,collectif tirage limite signe moebins 2007.

المواقع الالكترونية:

- الاتفاقية المتعلقة بالجريمة الالكترونية، بوداباست، مجلس أوروبا، مجموعة المعاهدات الأوروبية، رقم185، الموقع الرسمي لمجلس أوروبا <http://www.coe.int/web/cybercrime/home>
- التجارة الإلكترونية، الموسوعة السياسية، 2021، <https://political.encyclopedia.org/dictionary/>، أطلع عليه بتاريخ 2026/04/04، على الساعة 15:07 .

- Blog article: Crypto Mixer Money Laundering Is the Risk Worth the Reward? ,IDnow Houton Jody ,<https://www.idnow.io/blog/crypto-mixer-money-laundering-risk-reward/> ,Accessed March 27, 2026 ,time 23:30
- Blog article Chain-Hopping : The Defining Money Laundering Method of Modern Crypto Crime ,Elliptic , <https://www.elliptic.com/> ,Accessed March 30, 2026 ,time 22:04
- Blog article What Is DeFi in Crypto ,Cryptopolitan Nelluis irene ,august 2025 <https://www.cryptopolitan.com/ar/what-is-defi-in-crypto/?> , Accessed March 30, 2026 ,time 23:30
- Blog article ,Cybercrime and Virtual Economies in Online Gaming London: Royal United Services Institute (RUSI ,Anton Moiseienko and Kayla Izenman ,October 11, 2019 ,
https://static.rusi.org/20191011_newsbrief_vol39_no9_moiseienko_and_izenman_web.pdf?utm.com , Accessed March 30, 2026 ,time 23:30

