جامعة قاصدي مرباح – ورقلة
كلية الحقوق والعلوم السياسية
قسم الحقوق

مذكرة مقدمة لاستكمال المتطلبات لنيل شهادة الماستر أكاديمي/مهني

الميدان: الحقوق والعلوم السياسية

الشعبة: الحقوق

التخصص: قانون جنائي وعلوم جنائية

عنوان المذكرة

جرائم العملات الرقمية

إعداد الطالبتين: إشراف:

جريد مارية — أ. د محمد بن فردية

كيور الشائعة

أعضاء لجنة المناقشة

الاسم واللقب	الرتبة العلمية	الصفة
أ.د صالحي نجاة	أستاذ محاضر قسم "أ"	رئيسًا
أ. د محمد بن فردية	أستاذ التعليم العالي	مشرفًا ومقررا
أ.د بن عمر ياسين	أستاذ محاضر قسم "ب"	مناقشًا

السنة الجامعية: 2025 - 2026

جامعة قاصدي مرباح – ورقلة
كلية الحقوق والعلوم السياسية
قسم الحقوق

مذكرة مقدمة لاستكمال المتطلبات لنيل شهادة الماستر أكاديمي/مهني

الميدان: الحقوق والعلوم السياسية

الشعبة: الحقوق

التخصص: قانون جنائي وعلوم جنائية

عنوان المذكرة

جرائم العملات الرقمية

إعداد الطالبتين: إشراف:

جريد مارية أ. دمحمد بن فردية

كيور الشائعة

أعضاء لجنة المناقشة

الاسم واللقب	الرتبة العلمية	الصفة
أ.د صالحي نجاة	أستاذ محاضر قسم "أ"	رئيسًا
أ. د محمد بن فردية	أستاذ التعليم العالي	مشرفًا ومقررا
أ.د بن عمر ياسين	أستاذ محاضر قسم "ب"	مناقشًا

السنة الجامعية: 2025 - 2026

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة قاصدي مرباح - ورقلة

التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

(ملحق القرار الوزاري رقم 1082المؤرخ 27 ديسمبر 2020 الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها)

أنا الممضي أسفله،

إسم ولقب الطالب	التخصص	رقم بطاقة التعريف الوطنية	تاريخ الاصدار
1. جريد مارية	قانون جنائي	209176425	2023/ 05/02
2. كيور الشاعة	قانون جنائي	202322537	2018/01/29

المسجل (ة) بكلية الحقوق والعلوم السياسية قسم الحقوق

والمكلف (ة) بإنجاز أعمال بحث مذكرة ماستر عنوانها:

جرائم العملات الرقمية

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في انجاز البحث المذكور أعلاه.

التاريخ: 2026/05/15

1. توقيع المعني (ة) .
2. توقيع المعني (ة) .

شكر وعرفان

بسم الله الرحمن الرحيم ﴿ وَقُل رَبِّ زِدني عِلمًا ﴾

الحمد لله حمدًا كثيرًا طيبًا مباركًا فيه، الذي أنار لنا درب العلم والمعرفة، ووهبنا من فضله الصبر والإرادة، وأعاننا ووفقنا لإتمام هذا العمل المتواضع.

اعترافًا بالفضل لأهله، وعملًا بقول رسول الله ﷺ *"من لا يشكر الناس لا يشكر الله."*

يطيب لنا أن نتقدم بأسمى آيات الشكر، وأصدق عبارات الامتنان والتقدير إلى أستاذنا الفاضل والمشرف القدير **:الأستاذ محمد بن فردية** الذي تفضل بقبول إشرافه على هذه المذكرة الموسومة بـ " **:جرائم العملات الرقمية** ."لقد كان لسعة صدره، وتوجيهاته القيمة، ونصائحه السديدة، وملاحظاته الدقيقة الأثر البالغ في تذليل الصعاب وإثراء هذا البحث وإخراجه في هذه الحلة، فجزاه الله عنا خير الجزاء وأوفاه.

كما نتوجه بخالص الشكر ووافر الاحترام إلى كافة أساتذة قسم الحقوق، وتحديدًا أساتذة تخصص **القانون الجنائي والعلوم الجنائية** ، الذين نهلنا من معين علمهم طيلة مسيرتنا الجامعية ولم يبخلوا علينا بعطائهم المعرفي.

ويمتد شكرنا وتقديرنا إلى الأساتذة الأفاضل أعضاء لجنة المناقشة، لتفضلهم بقبول قراءة وتقييم وتقويم هذا العمل.

وأخيرًا، نتقدم بخالص الشكر لكل من مدّ لنا يد العون والمساعدة، سواء بالكلمة الطيبة، أو بتوفير المراجع، أو بتقديم الدعم المعنوي طيلة فترة إنجاز هذه المذكرة.

الإهداء

إلى أمي الغالية...

إلى النور الذي أضاء دربي، وإلى القلب الذي غمرني حبًّا وحنانًا ودعاءً لا ينقطع،

إليكِ يا من كان صبركِ وقوتكِ سببًا في وصولي إلى هذه اللحظة،

أهديكِ ثمرة جهدي المتواضع، عرفانًا بكل ما قدمتِه لي من تضحية ومحبة.

إلى إخوتي وأخواتي...

إلى من كانوا سندي بعد الله، وشاركوا معي لحظات التعب قبل الفرح،

شكرًا لدعمكم الدائم وكلماتكم التي كانت تمنحني القوة للاستمرار وتحقيق النجاح.

إلى أستاذي المشرف...

الذي كان خير موجّه وناصح، ولم يبخل عليّ بعلمه وتوجيهاته القيّمة،

أتقدم إليه بخالص الشكر والتقدير على صبره ومرافقته العلمية طوال إنجاز هذه المذكرة.

إلى نفسي...

التي صبرت واجتهدت وتجاوزت الصعوبات بإيمان وعزيمة،

حتى وصلت إلى هذه اللحظة التي أرجو أن تكون بداية لكل نجاح قادم.

إلى صديقتي رفيقة روحي ودربي والى كل من ساندني بدعوة صادقة أو كلمة طيبة،

أهدي هذا العمل المتواضع، راجيةً من الله التوفيق والسداد.

الطالبة

جريد مارية

الإهداء

بسم الله الرحمن الرحيموالصلاة والسلام على أشرف المرسلين وعلى آله وصحبه أجمعين

أُهدي ثمرة جهدي المتواضع:

إلى روح والدي الطاهرة (رحمه الله تعالى وأسكنه فسيح جناته)، الذي كان مثالاً للعطاء والتضحية، فأسأل الله أن يجعل هذا العمل صدقة جارية في ميزان حسناته.

وإلى أمي الغالية (حفظها الله وأطال في عمرها)، التي كانت ولا تزال مصدر الدعاء، والحنان، والصبر، فجزاها الله عني خير الجزاء.

وإلى زوجي الكريم، الأستاذ بجامعة ورقلة، الذي ساندني ووقف إلى جانبي بكل تشجيع طوال مسيرتي الدراسية.

وإلى إخوتي وأخواتي وعائلتي الأعزاء الذين ساندوني.

وإلى أبنائي وبناتي الأحبة الذين كانوا دافعاً لي للاستمرار والنجاح.

وإلى زميلتي في إعداد هذه المذكرة، شكراً على تعاونكِ وجهودكِ ومشاركتكِ القيّمة التي كانت سنداً في إنجاز هذا العمل مع خالص التقدير والاحترام.

كما أهدي هذا العمل إلى أحبتي وكل من رافقني بالدعاء والكلمة الطيبة والدعم الصادق.

وإلى أساتذتي الأفاضل الذين أناروا لنا طريق العلم والمعرفة، وخاصة أستاذي المحترم الذي أشرف على هذا العمل العلمي وأرشدنا بإرشاداته القيّمة، شكراً جزيلاً لك.

الطالبة كيور الشائعة

قائمة المختصرات

- ج.ر.ج.ح: الجريدة الرسمية للجمهورية الجزائرية
- ص: صفحة
- ط: طبعة
- ق.ع.ج:قانون العقوبات الجزائري
- مج: مجلة
- س : السنة
- ع: العدد

مقدمة

مقدمة

شهد العالم خلال السنوات الأخيرة تحولات عميقة في مجال المعاملات المالية نتيجة التطور السريع لتكنولوجيا الإعلام والاتصال، حيث لم تعد المبادلات الاقتصادية تعتمد فقط على النقود التقليدية أو الوسائل المصرفية المعروفة، بل ظهرت صور جديدة من الأصول الرقمية التي يتم تداولها عبر شبكات إلكترونية لا تخضع دائماً لرقابة مركزية مباشرة. وتُعد العملات الرقمية، ولا سيما العملات المشفرة، من أبرز هذه المستجدات، إذ تقوم على تقنيات معقدة كالتشفير وسلاسل الكتل، وتسمح بإجراء معاملات مالية سريعة وعابرة للحدود دون الحاجة إلى وسيط مصرفي تقليدي.

غير أن هذا التطور، رغم ما يحققه من مزايا في سرعة التعامل وانخفاض التكلفة وتسهيل المبادلات الرقمية، أفرز في المقابل تحديات قانونية وأمنية بالغة الأهمية. فقد أصبحت العملات الرقمية بيئة قابلة للاستغلال في ارتكاب أنماط إجرامية مستحدثة، مثل الاحتيال الرقمي، غسل الأموال، تمويل الأنشطة غير المشروعة، الاختراق الإلكتروني، وسرقة المحافظ الرقمية. وتزداد خطورة هذه الجرائم بالنظر إلى ما تتميز به العملات الرقمية من طابع لامادي، وصعوبة في تحديد هوية المتعاملين، وسرعة في نقل الأموال عبر الحدود، الأمر الذي يجعل مواجهتها بالوسائل القانونية التقليدية أمراً غير كافٍ في كثير من الحالات.

وتبرز **أهمية هذا الموضوع** من الناحية العلمية والعملية في كونه يعالج إشكالية قانونية حديثة تتصل بمدى قدرة المنظومة القانونية على استيعاب التطورات التقنية المتسارعة في المجال المالي الرقمي. فمن الناحية العلمية، يساهم الموضوع في ضبط المفاهيم القانونية المرتبطة بالعملات الرقمية وتمييزها عن النقود الإلكترونية والعملات الافتراضية. أما من الناحية العملية، فتظهر أهميته في بيان مدى فعالية القواعد الجنائية والإجرائية القائمة في مكافحة الجرائم المرتبطة بهذه العملات، خاصة في ظل صعوبات الإثبات، تتبع الأموال، تحديد الجناة، وتنازع الاختصاص القضائي.

وقد تناولت بعض **الدراسات السابقة** موضوع العملات الرقمية من زوايا متعددة، منها ما ركز على طبيعتها الاقتصادية والقانونية، ومنها ما تناول مخاطرها في غسل الأموال وتمويل الإرهاب، ومنها ما عالج الإشكالات التقنية المرتبطة بتتبعها وحجزها. غير أن هذه الدراسات، رغم أهميتها، لا تزال تترك مجالاً للبحث في مدى كفاية المنظومة القانونية لمواجهة الجرائم المرتبطة بالعملات الرقمية في ظل التطور السريع لأساليب الجناة والبيئة الرقمية العابرة للحدود .

ومن هنا **تهدف هذه الدراسة** إلى بيان الإطار المفاهيمي والقانوني للعملات الرقمية، وتحديد خصائصها التي تجعلها محلاً خاصاً للجريمة، ثم تحليل الأساس القانوني للمسؤولية الجنائية عن الأفعال

المرتبطة بها، وصولاً إلى دراسة أهم صور الجرائم التي تقع من خلالها، وبيان الآليات القانونية والقضائية والإجرائية المعتمدة لمواجهتها. كما تهدف الدراسة إلى إبراز مواطن القصور في النصوص الحالية، وبيان الحاجة إلى تطوير أدوات المكافحة بما ينسجم مع خصوصية الجريمة الرقمية.

وتنحصر **حدود هذه الدراسة** من الناحية الموضوعية في بحث الجرائم المرتبطة بالعملات الرقمية، دون التوسع في جميع الجوانب الاقتصادية أو التقنية لهذه العملات إلا بالقدر الذي يخدم التحليل القانوني. أما من الناحية المكانية، فتركز الدراسة أساساً على المنظومة القانونية الجزائرية، مع الاستئناس ببعض المواقف والتجارب المقارنة عند الاقتضاء. ومن الناحية الزمانية، ترتبط الدراسة بمرحلة التطور الحديث للعملات الرقمية وتزايد استعمالها في الأنشطة المشروعة وغير المشروعة.

وعلى ضوء ما سبق، تتمحور إشكالية هذه الدراسة حول السؤال الآتي:

ما مدى فعالية المنظومة القانونية في مواكبة التحديات المرتبطة بجرائم العملات الرقمية؟

وللإجابة عن هذه الإشكالية، تم الاعتماد على المنهج الوصفي من خلال عرض المفاهيم والخصائص المرتبطة بالعملات الرقمية، والمنهج التحليلي من خلال تحليل النصوص القانونية ذات الصلة وبيان مدى كفايتها في مواجهة الجرائم المستحدثة، مع الاستعانة بالمنهج المقارن كلما اقتضت الدراسة ذلك لإبراز بعض التجارب أو المواقف القانونية المقارنة.

وعليه، تم تقسيم هذه الدراسة إلى فصلين أساسيين؛ خُصص الفصل الأول لدراسة الإطار المفاهيمي والقانوني لجرائم العملات الرقمية، من خلال تحديد ماهية هذه العملات وخصائصها وتكييفها القانوني وأساس المسؤولية الجنائية المرتبطة بها. أما الفصل الثاني، فقد خُصص لدراسة صور الجرائم المرتبطة بالعملات الرقمية وآليات مكافحتها، من خلال بيان أهم الأنماط الإجرامية المستحدثة، ثم تحليل وسائل المواجهة القضائية والإجرائية والتقنية المعتمدة للحد من خطورتها .

الفصل الأول:الإطار المفاهيمي والقانوني لجرائم العملات الرقمية

لدراسة الجرائم المرتبطة بالعملات الرقمية من الناحية القانونية، لا بد أولاً من إزالة الغموض الذي يحيط بهذه الأصول المستحدثة. فالقاعدة الجنائية ترتبط ارتباطاً وثيقاً بطبيعة المحل الذي تقع عليه الجريمة، مما يفرض علينا ضبط ماهية هذه العملات وبيان خصائصها التي جعلتها بيئة جاذبة للنشاط الإجرامي. وعليه، قسمنا هذا الفصل إلى مبحثين:

المبحث الأول: التأصيل المفاهيمي للعملات الرقمية.

المبحث الثاني: الأساس القانوني للمسؤولية الجنائية.

المبحث الأول: التأصيل المفاهيمي للعملات الرقمية

قبل البحث في الجوانب الإجرائية والجزائية، من الضروري تحديد المقصود بالعملات الرقمية لغةً وقانوناً، لاسيما وأنها ظاهرة مالية وتقنية حديثة تتداخل مع مفاهيم أخرى كالنقود الإلكترونية والافتراضية. لذلك، سنعمل في هذا المبحث على توضيح هذا المفهوم بدقة، واستعراض الخصائص التقنية والاقتصادية التي تمنح هذه العملات طبيعتها اللامركزية. ونختتم المبحث بتتبع التكييف القانوني لهذه الأصول ومواقف التشريعات الوطنية والمقارنة منها، وذلك من خلال ثلاثة مطالب متتالية.

المطلب الأول: مفهوم العملات الرقمية وتميزها عن غيرها

تقتضي الدراسة المنهجية لجرائم العملات الرقمية ضبطاً دقيقاً لمفاهيمها الأساسية قبل التطرق لأحكامها الموضوعية والجزائية. وعليه، يهدف هذا المطلب إلى تحديد الماهية القانونية والتقنية لهذه العملات(الفرع الأول)، وبيان الفروق الجوهرية بينها وبين الأنظمة المالية المشابهة لها في البيئة الرقمية (الفرع الثاني)، وذلك لتفادي أي تداخل مفاهيمي أثناء معالجة الجرائم المرتبطة بها.

الفرع الأول: تعريف العملات الرقمية

تُعد العملات الرقمية من أبرز الإفرازات التكنولوجية المعاصرة التي ألقت بظلالها على الاقتصاد ومستقبل المعاملات المالية. وقبل التطرق لماهية هذه العملات، تجدر الإشارة إلى أن النقود التقليدية تُعرف بأنها: «كل شيء يلاقي قبولاً عاماً كوسيط للمبادلة ويستخدم لتسوية المدفوعات وإبراء الديون» [1]. وللإحاطة الشاملة بهذا المفهوم المستحدث، سنعرض فيما يلي التعريفات الفقهية والتشريعية التي حاولت ضبط ماهيته.

تمهيد:

لم تكن العملات الرقمية وليدة الصدفة، بل جاءت كمرحلة حتمية وطبيعية في مسار التطور التاريخي لظاهرة النقود؛ فالبشرية لم تعرف النقد في صورته الورقية أو المعدنية الحالية إلا بعد مخاض طويل بدأ بنظام المقايضة، ثم الانتقال إلى السلع الوسيطة كالذهب والفضة، وصولاً إلى النقود القانونية (الإلزامية) المدعومة من الدول والبنوك المركزية. ومع الثورة التكنولوجية المعاصرة وظهور شبكة الإنترنت

1 نذير عبد الرزاق، وحجاب عيسى، "وظائف النقود في الفكر الاقتصادي الإسلامي والاقتصاد الوطني دراسة مقارنة"، مجلة الحقوق والعلوم الإنسانية دراسات اقتصادية، مج. 07، ع. 02 س (2013).

في أواخر القرن العشرين، انتقل العالم من "مادية الاقتصاد" إلى "رقمية التعاملات"، وهو ما فتح الباب على مصراعيه للبحث عن صيغ نقدية تتلاءم مع هذه البيئة الافتراضية العابرة للحدود.

أولاً: التعريف الفقهي للعملات الرقمية

تعددت الاجتهادات الفقهية حول تعريف النقود الرقمية تبعاً لاختلاف الزاوية التقنية أو القانونية؛ فبينما ركز جانب من الفقه على البنية الفنية، عرّفها آخرون كأداة وفاء بديلة. وقد طُرحت عدة تعريفات تعتبر النقود الإلكترونية: «وحدات إلكترونية يتم انتقالها بطريقة معينة من حساب شخص إلى حساب شخص آخر، حيث تخزن هذه الوحدات إما في ذاكرة كمبيوتر صغير ملتصق في كارت يحمله المستهلك... أو تخزن في ذاكرة الكمبيوتر الشخصي». [1]

كما نُظر إليها من منظور تقني بحت على أنها مجموعة من البروتوكولات والتوقيعات الرقمية التي تتيح للرسالة الإلكترونية الحلول محل العملات التقليدية. وفي محاولة لضبط خصائصها الاستعمالية، عُرفت بأنها قيمة نقدية مخزنة على وسيلة إلكترونية، مدفوعة مقدماً وغير مرتبطة بحساب بنكي، وتحظى بقبول واسع من غير مصدرها كأداة للدفع.

ويوسع الفقه من دائرة هذا المفهوم ليشمل كل عملة، أو أصل شبيه بالمال، تتم إدارته أو تخزينه أو تبادله بشكل أساسي عبر أنظمة الكمبيوتر وشبكة الإنترنت، سواء تم حفظها في قواعد بيانات مركزية تابعة لمؤسسات مالية، أو عبر قواعد بيانات لامركزية وموزعة (البلوك تشين). وخلاصة هذه الاتجاهات الفقهية أن النقود الإلكترونية هي المكافئ الرقمي للنقود التقليدية، وتتمثل في قيمة نقدية إلكترونية مدفوعة مسبقاً، يحوزها المستهلك للوفاء بمختلف الالتزامات النقدية.

ثانياً: التعريف التشريعي (الدولي والوطني)

لم تكتفِ المنظمات الدولية والمشرعون الوطنيون بالتعريفات الفقهية، بل سعوا لإيجاد تعريفات قانونية تضبط نطاق الرقابة والعقاب.

1. على المستوى الدولي والمقارن: عرّف مؤتمر بازل (1998) النقود الإلكترونية بأنها القيمة المخزونة أو آليات الدفع المدفوعة مسبقاً لتنفيذ الدفعات عبر أجهزة بيع خاصة أو شبكات الحاسوب المفتوحة كالإنترنت. من جانبه، قدم البنك المركزي الأوروبي تعريفاً أكثر دقة، واصفاً إياها بأنها:

1 يُغربي حمزة، وبدروني عيسى، "العملات المشفرة النشأة التطور والمخاطر"، مجلة الدراسات الاقتصادية معاصرة، مج. 05، ع. 02 س (2020) ص 69-70.

«مخزون إلكتروني لقيمة نقدية على وسيلة تقنية يستخدم بصورة شائعة للقيام بمدفوعات المتعهدين غير من أصدرها، دون الحاجة لوجود حساب بنكي عند إجراء الصفقة». [1]

أما المشرع الفرنسي، فقد نص في المادة L315-1 من قانون النقد والمالية (المعدل عام 2013) على أن النقود الإلكترونية هي قيمة نقدية مخزنة في شكل إلكتروني (بما في ذلك المغناطيسي)، تمثل مطالبة على المصدر، وتصدر مقابل تحويل الأموال لغرض معاملات الدفع. [2]

2. على مستوى التشريع الجزائري: تبنى المشرع الجزائري مفهوماً مرناً لوسائل الدفع لاستيعاب التطور التقني، حيث نصت المادة 69 من قانون النقد والقرض (03-11) على أنه: «تعتبر وسائل دفع كل الأدوات التي تمكن كل شخص من تحويل أموال مهما كان السند أو الأسلوب المستعمل». كما عزز قانون التجارة الإلكترونية هذا الاتجاه بتعريف وسيلة الدفع الإلكترونية في المادة 06 بأنها كل وسيلة مرخص بها تمكن صاحبها من القيام بالدفع عن قرب أو عن بعد عبر منظومة إلكترونية. [3]

غير أن المشرع الجزائري اتخذ موقفاً حازماً وحذراً تجاه "العملات الافتراضية" (غير المركزية)، حيث نصت المادة 117 من قانون المالية [4] لسنة 2018 صراحة على منع شراء أو بيع أو استعمال أو حيازة العملة الافتراضية، وعرّفتها بأنها: «تلك التي يستعملها مستخدمو الإنترنت عبر الشبكة العنكبوتية، وهي تتميز بغياب الدعامة المادية كالقطع والأوراق النقدية وعمليات الدفع بالصك أو بالبطاقة البنكية». ويعود هذا الحظر التشريعي الصارم إلى غياب السلطة الرقابية على هذه العملات، وتخوف الدولة من استغلالها في المتاجرة بالمخدرات وتبييض الأموال والتهرب الضريبي. [5]

---

1 حبيبة عبدلي، ونور الدين موفق، "تبييض الأموال في البيئة الإلكترونية"، المؤتمر الدولي الافتراضي لمكافحة الفساد في البيئة الإلكترونية (برلين: المركز الديمقراطي العربي، س (2021)، ص 63.

2Haroon Al-Tarawneh, Najwan Abdallat & Mohamad Al-Laham, "Development of Electronic Money and Its Impact on the Central Bank Role and Monetary Policy," Issues in Informing Science and Information Technology 6 (2009) p ,p 340-341.

3 عثمان عثمانية، ووداد بن قيراط، *اقتصاد العملات المشفرة ومستقبل النقود* (المركز العربي للأبحاث ودراسة السياسات، بيروت 2022)، ص 86.

4 قانون رقم 17-11 مؤرخ في 27 ديسمبر سنة 2017، يتضمن قانون المالية لسنة 2018، الجريدة الرسمية للجمهورية الجزائرية، العدد 76، الصادر بتاريخ 28 ديسمبر 2017، المادة 117.

5 زكرياء مسعودي، وطاد الزهرة جقريف، " *ماهية النقود الإلكترونية* "، المجلة الدولية للبحوث القانونية والسياسية، مج. 02، ع. 03 (ديسمبر 2018):ص 40-41.

الفرع الثاني: تمييز العملات الرقمية عن النقود الإلكترونية

يثير التقارب التقني بين العملات الرقمية والنقود الإلكترونية لبساً يستوجب التمييز الدقيق بينهما، فرغم اشتراكهما في الطبيعة الرقمية والخلو من الكيان المادي، إلا أنهما يختلفان جذرياً من حيث الطبيعة القانونية واليات العمل. ولفهم هذا التباين، يجب أولاً تحديد المفهوم القانوني للنقود الإلكترونية؛ إذ ووفقاً للتوجيه الأوروبي،تعرف النقود الإلكترونية بأنها قيمة نقدية تمثل ديناً على المصدر، تخزن إلكترونياً، وتصدر مقابل تسلم أموال لا تقل قيمتها عن القيمة النقدية المصدرة، وتقبل كوسيلة للدفع من قبل مؤسسات أخرى غير الجهة المصدرة "

بناء على هذا الإطار، يكمن الفارق الجوهري الأول في وحدة الحساب والارتباط بالنقود التقليدية. فالنقود الإلكترونية تحافظ على ارتباطها الوثيق بالعملات التقليدية المتمتعة بقوة الإبراء القانونية (مثل الدولار أو اليورو)، وتعبر عن القيمة ذاتها، مما يمنحها غطاءقانونياً يضمن للمستخدم استرداد أمواله بنفسالقيمة

في المقابل، تعتمد العملات الرقمية والافتراضية على وحدات حساب مبتكرة ومستقلة (مثل البيتكوين)، وتفتقر إلى صفة العملة القانونية، وتتحدد قيمتها بناءً على قوى العرض والطلب، مما يجعل عملية تحويلها أو استردادها محفوفة بالتقلبات وغير مضمونة القيمةمن الناحية القانونية والرقابية، تخضع النقود الإلكترونية لتنظيم تشريعي صارم، وتصدرها مؤسسات مالية معتمدة قانوناً تخضع لرقابة وإشراف السلطات النقدية المركزية لضمان استقرارها وحماية المتعاملين بها على النقيض من ذلك، تعمل غالبية العملات الرقمية خارج مظلة التنظيم القانوني، وتصدرها جهات خاصة غير مالية أو تعتمد على برمجيات اللامركزية، مما يجعلها بمنأى عن أي إشراف حكومي أو رقابة احترازية، وينعكس هذا على المعروض النقدي؛ ففي حين يكون المعروض من النقود الإلكترونية ثابتاً وموازياً لما تم إبداعه من أموال تقليدية، فإن المعروض من العملات الرقمية غير ثابت ويرتبط بقرارات مصدريها أو خوارزميات برمجتهاوأخيراً، ينعكس هذا التباين الهيكلي والقانوني بشكل مباشر على طبيعة المخاطر المرتبطة بكل نظام، إذ تنحصر المخاطر التي تواجه النقود الإلكترونية أساساً في المخاطر التشغيلية المتعلقة باحتمالية تعطل الأنظمة الإلكترونية الحافظة لها، أما العملات الرقمية، ونظراً الغياب الإطار القانوني والرقابة العامة، فإنها تواجه

حزمة معقدة من المخاطر تتعدى الجانب التشغيلي لتشمل المخاطر القانونية، ومخاطر الائتمان، ومخاطر السيولة، فضلاً عن ارتفاع احتمالية التعرض للاحتيال المالي .[1]

الفرع الثالث: تمييز العملات الرقمية عن العملات الافتراضية

يُشكل مصطلح "العملات الرقمية" المظلة الكبرى التي تنطوي تحتها كافة أشكال الأموال في البيئة الإلكترونية، في حين تُمثل "العملات الافتراضية" تطبيقاً خاصاً ضمن هذه المظلة. ولتمييز العملات الافتراضية بدقة، تتجه المنظمات الدولية، وفي طليعتها مجموعة العمل المالي (FATF) ، إلى تقسيمها هيكلياً ووظيفياً بناءً على معياري قابلية التحويل والمركزية، بعيداً عن الغطاء القانوني الإلزامي الذي قد تتمتع به بعض العملات الرقمية الأخرى.

يتجلى معيار قابلية التحويل في انقسام العملات الافتراضية إلى أنظمة مغلقة وأخرى مفتوحة. فالعملات الافتراضية غير القابلة للتحويل (الأنظمة المغلقة) صُممت لتعمل حصرياً داخل نطاقات أو عوالم افتراضية محددة، مثل الألعاب الإلكترونية الجماعية، وتخضع لقواعد تمنع قانوناً استبدالها بالعملات النقدية التقليدية الإلزامية. في المقابل، تمتلك العملات الافتراضية القابلة للتحويل (الأنظمة المفتوحة) قيمة معادلة في العالم الحقيقي ويمكن تبادلها بالنقود التقليدية، غير أن هذه القابلية للتحويل ليست مضمونة بقوة القانون أو بدعم من سلطة نقدية، بل هي قابلية تحويل واقعية (De facto) تفرضها قوى العرض والطلب في الأسواق الخاصة.

أما المعيار الثاني للتمييز فيكمن في هيكل الإدارة والمركزية؛ إذ تتسم كافة العملات الافتراضية غير القابلة للتحويل بالمركزية المطلقة، حيث تصدرها وتديرها جهة واحدة تضع قواعد عملها وتتحكم في سجلات الدفع الخاصة بها. وعلى النقيض من ذلك، تتنوع العملات الافتراضية القابلة للتحويل بين أنظمة مركزية، وأنظمة لامركزية تُعرف اصطلاحاً بـ "العملات المشفرة .(Cryptocurrencies) "وتتميز هذه الأخيرة، مثل عملة البيتكوين(Bitcoin) ، باعتمادها على برمجيات مفتوحة المصدر وبروتوكولات رياضية وتشفيرية معقدة لضمان أمان التحويلات بين النظراء (Peer-to-peer) دون الحاجة لأي سلطة إدارية أو رقابية مركزية[2]

1 -زكريا مسعودي نفس المرجع ص ص 42-43

2Financial Action Task Force (FATF), Virtual Currencies: Key Definitions and Potential AML/CFT Risks (Paris: FATF, 2014),p 4-7

يتضح مما سبق أن الفارق الجوهري يكمن في النطاق والتنظيم؛ فبينما قد تشمل العملات الرقمية عموماً أشكالاً منظمة ومُصدرة من بنوك مركزية، تنحصر العملات الافتراضية في كونها ابتكاراً تقنياً خاصاً، إما أن يكون حبيس بيئات إلكترونية مغلقة، أو يتخذ شكلاً مشفراً ولامركزياً يفتقر إلى أي صفة قانونية إلزامية أو غطاء سيادي، مما يجعله بيئة خصبة للعديد من التحديات والمخاطر القانونية.

يتضح من خلال ما سبق دراسته أن العملات الرقمية تختلف جذرياً عن كل من النقود الإلكترونية والعملات الافتراضية. فهي تفتقر للغطاء النقدي والرقابة القانونية المؤسسية التي تحظى بها النقود الإلكترونية، وتتجاوز في نطاق استخداماتها البيئات المغلقة التي تميز العملات الافتراضية. وهذا التباين، مقترناً بغياب التنظيم التشريعي الموحد، هو ما يضفي على العملات الرقمية طبيعة خاصة ومخاطر متعددة، وهو ما سيتم تفصيله في المطلب الموالي المخصص لدراسة خصائصها.

المطلب الثاني: خصائص العملات الرقمية

تتميز العملات الرقمية بخصائص تقنية وذاتية تجعلها مختلفة عن النقود التقليدية ووسائل الدفع الإلكترونية. فهي تقوم على اللامركزية والتشفير وغياب الوسيط، مما يمنحها سرعة في التداول وصعوبة في الرقابة. وعليه، سنتناول في هذا المطلب الخصائص التقنية في(الفرع الأول)، والخصائص الذاتية في (الفرع الثاني).

الفرع الأول: الخصائص التقنية

تتميز العملات المشفرة، باعتبارها التطبيق الأبرز للعملات الرقمية، بطبيعة إلكترونية بحتة خالية من أي كيان مادي، حيث تُحفظ في محافظ رقمية (Digital Wallets) لا تخضع لسلطة المؤسسات المصرفية. وترتكز هيكليتها التقنية بشكل أساسي على مبدأ اللامركزية (Decentralized Control) وغياب الوسيط؛ إذ تعمل وفق نظام شبكة الند للند (Peer-to-Peer) ، مما ينفي الحاجة إلى وجود طرف ثالث موثوق كالبنوك أو الحكومات لإدارة التحويلات. هذا البناء التقني المستقل والمبني على برمجيات مفتوحة المصدر (Open-Source) ، يمنح النظام مرونة في التطوير ويجعله متحرراً من قيود السياسات النقدية التقليدية وتحكم السلطات المركزية في المعروض النقدي.[1]

1Prasad, E., and Ye, L., The Renminbi Prospects as a Global Reserve Currency, Cato Journal, 33(3), 2013, pp. 563-570 .

ولتعويض غياب السلطة الرقابية المركزية، تعتمد هذه العملات على خوارزميات تشفير رياضية معقدة لضمان أمان الشبكة. يتم ذلك عبر استخدام مفاتيح غير متماثلة (مفتاح عام كعنوان، ومفتاح خاص كتوقيع سري) تضمن حماية المعاملات. والمفارقة التقنية الجوهرية هنا تكمن في الجمع بين الشفافية والسرية؛ فبينما تُسجل كافة المعاملات علناً في دفتر أستاذ عام يُعرف بسلسلة الكتل (Blockchain)يتيح للجميع تتبع حركة الأموال، تبقى الهوية الحقيقية للمتعاملين مخفية خلف أسماء مستعارة (Pseudonymity) تتمثل في عناوين أبجدية رقمية. ورغم وجود أدوات لزيادة إخفاء الهوية مثل برامج (Tor) أو "الخلاطات(Mixers) "، فإن هذه الميزة تثير إشكاليات قانونية جسيمة فيما يتعلق بتحديد هوية أطراف التعامل.[1]

من جهة أخرى، تعالج الشبكة اللامركزية إشكالية "الإنفاق المزدوج – (Double-spending) " المتمثلة في خطر استنساخ الوحدة الرقمية واستخدامها أكثر من مرة – عبر توكيل مهمة التحقق وتدقيق المعاملات إلى مجموعة من مستخدمي الشبكة يُطلق عليهم "المُعدّنون .(Miners) "يقوم هؤلاء بتسخير قدرات حواسيبهم لحل معادلات رياضية معقدة بغرض التحقق من دقة التحويلات وتوثيقها في سلسلة الكتل.[2]

وفي مقابل جهودهم في حماية الشبكة، يُكافأ المُعدّنون بوحدات جديدة من العملة فيما يُعرف بعملية "التعدين .(Mining) "وتعد هذه العملية المصدر التقني الوحيد لسك عملات جديدة وضخها في التداول وفق سقف أقصى محدد مسبقاً برمجياً (مثل الحد الأقصى للبيتكوين البالغ 21 مليون وحدة)، مما يضفي عليها خاصية الندرة ويحد من التحكم العشوائي في عرضها.[3]وتنعكس هذه المنظومة المتكاملة على كفاءة المعاملات، فغياب الوسطاء والاعتماد على النقل الإلكتروني المباشر عبر الحدود يجعل من العملات المشفرة وسيلة تتسم بالسرعة الفائقة وانخفاض تكلفة التحويل مقارنة بنظم الدفع الإلكترونية التقليدية.[4]

---

1 طه مصطفى كمال وبندق، وائل أنور، الأوراق التجارية الإلكترونية ووسائل الدفع الإلكترونية الحديثة، دار الفكر الجامعي، الإسكندرية، مصر، 2010، ص 346

2Fratzscher, M., & Mehl, A., China's Dominance Hypothesis and the Emergence of a Tri-polar Global Currency System, The Economic Journal, 124(581), 2014, p. 1350.

3 فتحي الحموري، ناهد، الأوراق التجارية الإلكترونية، الطبعة 2، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2010، ص 113.

4 لبيب ابراهيم أحمد السيد، الدفع بالنقود الإلكترونية الماهية والتنظيم القانوني: دراسة تحليلية مقارنة، دار الجامعة الجديدة، الإسكندرية، 2009، ص 36.

الفرع الثاني: الخصائص الذاتية

تتسم العملات المشفرة، إلى جانب بنيتها التقنية، بجملة من الخصائص الذاتية والاقتصادية التي تفصلها تماماً عن المفهوم الكلاسيكي للنقود. وتبرز في مقدمة هذه الخصائص الاستقلالية التامة عن الإصدار السيادي؛ فهذه العملات لا تصدر عن أي دولة أو سلطة نقدية مركزية، ولا تخضع لأدوات الرقابة الحكومية التي تضبط حركة تداول الأموال. بل إن الفلسفة الأساسية التي استندت إليها نشأة هذه العملات هي التحرر من هيمنة الحكومات على النظام المالي العالمي، وخلق بيئة تداول مستقلة خارج نطاق الرقابة المصرفية التقليدية.[1]

ويرتبط بهذا التحرر المالي خاصية جوهرية أخرى تتمثل في انعدام الغطاء المادي أو القانوني. فالنقود التقليدية تستمد قوتها الإبرائية وموثوقيتها من سلطة الدولة وضمانها (سواء بغطاء من المعادن النفيسة كالذهب أو بقوة القانون)، في حين تفتقر العملات المشفرة لأي غطاء مادي يضمن استقرار قيمتها. وتتحدد قيمة هذه العملات حصرياً بناءً على آليات السوق (قوى العرض والطلب) وثقة المتعاملين في الشبكة. ورغم غياب هذا الضامن الرسمي أو المؤسسي، فإنها تحتفظ بقابليتها للتحويل إلى نقود قانونية، وتُستخدم فعلياً كوسيط في التجارة الإلكترونية وتسوية المدفوعات

علاوة على ذلك، تسبغ هذه العملات على مستخدميها طابعاً من السرية المالية والخصوصية الفائقة. فالمحافظ الرقمية تعمل في منأى تام عن أي سلطة رقابية أو مؤسسة مالية قد تطلب الإفصاح عن البيانات. ورغم أن جميع التحويلات تُسجل علناً في السجل العام (البلوك تشين)، إلا أن هذا التسجيل يقتصر على الرموز والأرقام المشفرة للمحافظ دون أدنى إشارة للأسماء أو الهويات الحقيقية لأطراف المعاملة. هذه السرية المطلقة للذمة المالية، وانعدام القدرة التقنية المباشرة على كشف هوية المتعاملين، تشكل خروجاً صريحاً عن قواعد الشفافية المفروضة في الأنظمة المصرفية، وتطرح تحديات قانونية جسيمة أمام جهات إنفاذ القانون[2]

الفرع الثالث: مزايا ومخاطر العملات الرقمية ومجالات استخدامها

1 سمر محمد أحمد علي، العملات الافتراضية المشفرة (ماهيتها، وخصائصها، ووضعها القانوني)، مجلة جامعة جنوب الوادي الدولية للدراسات القانونية، العدد الثامن، مصر، 2025، ص 279-281.

2 سمر محمد أحمد علي، مرجع سبق ذكره، 2025، ص 280-281.

أفرز التطور المتسارع للعملات المشفرة وتوسع مجالات استخدامها – سواء في التجارة الإلكترونية، أو التحويلات المالية عبر الحدود، أو كأدوات استثمارية – جملة من المزايا التي دفعت ببعض الأنظمة إلى محاولة تقنينها. وتتجسد أبرز هذه الإيجابيات في سرعة وسلاسة إنجاز المعاملات وانخفاض تكلفتها، وذلك لانتفاء الحاجة للوسطاء الماليين التقليديين. كما توفر هذه العملات بيئة تعامل آمنة بفضل تقنيات التشفير المعقدة، مقترنة بمستوى عالٍ من الشفافية في تتبع مسار الأموال عبر السجل العام، مع الاحتفاظ في الوقت ذاته بسرية هويات المتعاملين، وهو ما يقلل من مخاطر اختراق البيانات الشخصية المرتبطة بوسائل الدفع الإلكترونية الكلاسيكية.

على النقيض من ذلك، يطرح هذا الاستخدام المتزايد مخاطر وتحديات جسيمة تهدد الاستقرار المالي والاقتصادي للدول. فمن الناحية النقدية والجبائية، يؤدي غياب الرقابة المركزية واستخدام الأسماء المستعارة إلى إضعاف سيادة الدولة على سياستها النقدية، وخلق صعوبات بالغة في ضبط التدفقات المالية وحساب المجمعات النقدية. كما تعيق هذه السرية آليات التحصيل الضريبي، مما يعمق من ظاهرة الاقتصاد الخفي ويسهل التهرب الجبائي. ومن الناحية الاقتصادية، تساهم الطبيعة المتقلبة لهذه العملات في توسيع الفجوة بين الاقتصاد الحقيقي والاقتصاد المالي نتيجة تحولها إلى أداة للمضاربة البحتة، فضلاً عن غياب آليات حماية المستهلك في حالات القرصنة أو فقدان مفاتيح الوصول للمحافظ الرقمية، لعدم وجود سلطة تحكيم مركزية تلزم بتعويض المتضررين.

ولا تقتصر تداعيات العملات المشفرة على الجانب الاقتصادي البحت، بل تتعداه لتشكل بيئة خصبة لجرائم غسل الأموال وتمويل الأنشطة غير المشروعة. فالطبيعة العابرة للحدود لهذه المعاملات، وتمركز العديد من منصات التداول في ملاذات مالية خارجية، تعيق جهود الأجهزة الرقابية في تتبع مصادر الأموال وتخلق ثغرات عميقة في تطبيق قوانين مكافحة غسل الأموال. وعلاوة على ما سبق، تبرز المخاطر البيئية الناجمة عن عملية "التعدين" كأحد أخطر التداعيات، حيث تتطلب هذه العملية طاقة حاسوبية ضخمة تستهلك كميات هائلة من الموارد الطبيعية والكهرباء، مما يفاقم من الانبعاثات الكربونية ويشكل تهديداً ملموساً للسلامة البيئية، بتكاليف صحية وبيئية قد توازي أو تفوق القيمة السوقية للعملة ذاتها.[1]

1 عابد صونية، العملات الرقمية والاستقرار المالي: المزايا والمخاطر والتحديات، مداخلة مقدمة في الملتقى الدولي حول العملات الرقمية وتحديات الأمن السيبراني، جامعة طاهري محمد، بشار، الجزائر، 20-21 نوفمبر 2024، ص 11-17.

المطلب الثالث: التكييف القانوني للعملات الرقمية

يثير التكييف القانوني للعملات الرقمية تبايناً فقهياً وتشريعياً واسعاً، نظراً لتعارض طبيعتها اللامركزية مع المفهوم التقليدي للسيادة النقدية للدول. ولتأطير هذه الظاهرة، تباينت استجابات النظم القانونية بين الحظر المطلق، والتنظيم المرن، ومحاولة إيجاد ضمانات دولية موحدة.

الفرع الأول: الموقف التشريعي الوطني والمقارن (النصوص القانونية)

لم تتخذ التشريعات المقارنة موقفاً موحداً إزاء التكييف القانوني للعملات المشفرة، بل انقسمت توجهاتها وفقاً للسياسات الاقتصادية والأمنية لكل دولة. ففي الاتجاه التنظيمي المرن، سارعت المصلحة التشريعية والضريبية في دولة ألمانيا الاتحادية إلى الاعتراف التدريجي بالعملات المشفرة (كالبيتكوين) كأداة مالية قابلة للتداول، وأخضعتها للتنظيم الجبائي من خلال فرض ضرائب على الأرباح التجارية للشركات المتعاملة بها، مع إقرار إعفاءات ضريبية على المعاملات الفردية لتشجيع الابتكار الرقمي.[1]

وفي الاتجاه المتبني للتكنولوجيا اللامركزية، سعت دولة الإمارات العربية المتحدة إلى توظيف تقنية سلسلة الكتل (البلوك تشين) ضمن بنيتها التحتية المؤسسية. ورغم حذرها من العملات المشفرة المفتوحة، تبنت استراتيجية تعتمد على شبكات "بلوك تشين" مغلقة (PrivateBlockchain) لضمان أمن البيانات، وتوجت هذا المسار بمبادرات لإطلاق عملات رقمية حكومية(مثل مبادرة Em Cash في دبي)لتسهيل المدفوعات الرسمية والتجارية تحت غطاء قانوني محلي.[2]

وعلى النقيض من ذلك، برز الاتجاه التشريعي الحظري، والذي تزعمته دول رائدة اقتصادياً كجمهورية الصين الشعبية. فرغم استحواذها على النسبة الأكبر من قدرات التعدين عالمياً، أقرت الحكومة الصينية سلسلة من اللوائح التنظيمية الصارمة وصولاً إلى حظر وتجريم عمليات التعدين والتداول المفتوح،

1 منصور علي منصور شطا، العملات الافتراضية المشفرة وأثرها على مستقبل المعاملات (الواقع وآفاق المستقبل)، مجلة كلية الشريعة والقانون بطنطا، جامعة الأزهر، العدد السابع والثلاثون، الجزء الأول، مصر، 2022، ص 1842.

2 علي محمد الخوري، المدفوعات الإلكترونية والعملات الرقمية، مجلس الوحدة الاقتصادية العربية بجامعة الدول العربية، الإمارات العربية المتحدة، 2021، ص 131–132. وكذا: عاصم عادل محمد العضايلة، العملات الرقمية الافتراضية، طريق لتمويل الإرهاب، مجلة جامعة الزيتونة الأردنية للدراسات القانونية، المجلد 1، العدد 1، الأردن، 2020، ص 40.

وذلك حماية لسيادتها النقدية، مع الإبقاء على سعيها الحثيث لاحتكار تكنولوجيا البلوك تشين لبناء عملتها الرقمية السيادية الخاصة.[1]

أما في النظام القانوني الجزائري، فقد تبنى المشرع موقفاً حاسماً وحذراً، تجلى صراحة في المادة 117 من قانون المالية لسنة 2018، والتي نصت على المنع البات والمطلق لشراء العملات الرقمية الافتراضية، أو بيعها، أو حيازتها، أو تداولها. غير أن هذا المنع القانوني للعملات المشفرة اللامركزية لا ينفي التوجه الرسمي نحو التحديث المالي؛ إذ تتجه السلطات النقدية ممثلة في بنك الجزائر نحو دراسة إرساء إطار قانوني وتقني لإصدار عملة رقمية مركزية سيادية تحت مسمى "الدينار الرقمي الجزائري"، لتكون خاضعة تماماً للرقابة الرسمية.

الفرع الثاني: المواقف والضمانات القانونية الدولية

نظراً للطبيعة العابرة للحدود التي تتميز بها العملات المشفرة، فإن النصوص القانونية الوطنية تبقى قاصرة عن توفير حماية قانونية متكاملة مالم تُدعم بإطار تنظيمي دولي. وفي هذا السياق، لم ترقَ المواقف الدولية بعد إلى مصاف "الاتفاقيات الدولية الملزمة"، بل تجسدت في شكل توصيات ومبادرات(Soft Law)من أبرزها مبادرة المنتدى الاقتصادي العالمي (منتدى دافوس) بإنشاء "المجلس العالمي لحوكمة العملات الرقمية"، والذي يضم بنوكاً مركزية ومؤسسات مالية دولية، ويهدف إلى صياغة إطار عمل شامل ومتين يضبط حوكمة هذه العملات وينظم تداولها العالمي [2]

ويؤكد الفقه القانوني على ضرورة تفعيل ضمانات قانونية دولية لمعالجة الفراغ التشريعي وتوحيد الجهود، خاصة فيما يتعلق بمكافحة جرائم غسل الأموال والتهرب الضريبي. ويُقترح في هذا الصدد الاسترشاد بالنماذج التنظيمية القائمة في القطاع المصرفي، كتوصيات لجنة بازل للرقابة المصرفية (B.C.B.S)، أو المقاربات التشريعية للبنك المركزي الأوروبي في تجربة "اليورو الرقمي". إذ من شأن هذه الآليات أن تساهم في بلورة اتفاقيات دولية تضمن شفافية التعاملات، وتحمي الخصوصية دون أن

1See: Alice Ekman, China's Blockchain and Cryptocurrency Ambitions the first mover advantage, European Union Institute for Security Studies (EUISS), 2021, pp. 3-6.

2 علي محمد الخوري، المرجع السابق، ص 125.

تجعلها ذريعة للإفلات من العقاب، محققة بذلك التوازن بين متطلبات السرعة والائتمان الرقمي من جهة، والرقابة القانونية من جهة أخرى.[1]

المبحث الثاني: الأساس القانوني للمسؤولية الجنائية في جرائم العملات الرقمية

بعد أن أرسينا الإطار المفاهيمي والتنظيمي للعملات الرقمية، وحددنا طبيعتها وخصائصها الاستثنائية، ننتقل في هذا المبحث إلى معالجة الشق الجزائي المرتبط بها. فالاستخدام غير المشروع لهذه التقنيات المالية في البيئة الرقمية يستوجب قيام المسؤولية الجنائية، وهو ما يتطلب بدوره خضوع هذه الأفعال المحدثة للقواعد العامة للتجريم والعقاب. وللإلمام بهذا الأساس القانوني، يتعين علينا أولاً تفصيل الأركان العامة التي تقوم عليها الجريمة في البيئة الرقمية، ثم الانتقال لاحقاً لمعالجة إشكالية الإثبات الجنائي وحجية الأدلة المستمدة من هذه البيئة، وصولاً إلى تحديد قواعد الاختصاص القضائي.

المطلب الأول: أركان الجريمة في البيئة الرقمية

لا تخرج الجرائم المرتكبة في البيئة الرقمية، ومن ضمنها جرائم العملات المشفرة، عن القواعد العامة للقانون الجنائي من حيث وجوب توافر أركان الجريمة. لقيام أي جريمة إلكترونية، يستلزم القانون تضافر ثلاثة أركان أساسية: (الركن الشرعي) الذي يجسد مبدأ شرعية الجرائم والعقوبات، (الركن المادي) الذي يمثل المظهر الخارجي للسلوك الإجرامي، و(الركن المعنوي) الذي يعكس إرادة وعلم الجاني. وسيتم تفصيل هذه الأركان في الفروع الآتية.

الفرع الأول: الركن الشرعي

يُقصد بالركن الشرعي ضرورة تدخل المشرع لتجريم الأفعال الضارة بموجب نص قانوني صريح يحدد ماهية الفعل المحرم والعقوبة المقررة له، تكريساً لمبدأ "لا جريمة ولا عقوبة ولا تدبير أمن إلا بنص "[2] وفي مواجهة التطور التكنولوجي، تدخل المشرع الجزائري لسد الفراغ التشريعي عبر إيراد قسم خاص بجرائم "المساس بأنظمة المعالجة الآلية للمعطيات". تجسد ذلك في القسم السابع مكرر، والذي تضمن المواد من 394 مكرر إلى 394 مكرر 7، بموجب القانون رقم 04-15. ولم يكتفِ المشرع بذلك، بل

1 لافي محمد درادكة، تحديات مواكبة التنظيم القانوني للتطور التكنولوجي للعمل المالي والمصرفي، مجلة كلية القانون الكويتية العالمية، ملحق خاص، العدد 3، الجزء الأول، مايو 2018، ص 350-351. وكذا: محمد الشافعي، النقود الإلكترونية، ماهيتها مخاطرها وتنظيمها القانوني، مجلة الأمن والقانون، أكاديمية شرطة دبي، العدد 1، 2004، ص 19.

2 أحسن بوسقيعة، الوجيز في القانون الجزائي العام، الطبعة 10، دار هومة، الجزائر، 2011، ص 27.

أسبغ حماية جنائية على الحياة الخاصة للأفراد في مواجهة الاستخدام السيئ للتكنولوجيا عبر القانون رقم 06-23، والذي عدّل المادة 303 واستحدث المادة 303 مكرر 3. ويتقاطع هذا التوجه مع مسار المشرع الفرنسي الذي تدخل بنصوص صريحة للتحريم، مفصلاً بين جرائم الاعتداء على أنظمة المعالجة الآلية من جهة، وجريمتي تزوير المستندات المعالجة آلياً واستعمالها من جهة أخرى[1]

وقد أثار هذا التدخل التشريعي جدلاً فقهياً واسعاً حول المنهجية الأنسب لإدماج هذه النصوص في المنظومة العقابية. فانقسم الفقه إلى اتجاهات عدة؛ نادى الأول بإدماجها ضمن جرائم الأموال بناءً على إمكانية إضفاء صفة "المال" على الكيانات المادية والمعنوية للحاسوب. وفضل اتجاه ثانٍ إدراجها ضمن الجرائم الواقعة على الملكية، معتبراً الكيان المادي قابلاً للتملك والكيان المعنوي خاضعاً للملكية الفكرية. في حين ذهب اتجاه ثالث إلى ضرورة إفراد باب مستقل للجرائم المعلوماتية نظراً لطبيعتها الاقتصادية الخاصة. واستقر اتجاه رابع على ضرورة إلحاق كل جريمة معلوماتية بما يقابلها في قانون العقوبات التقليدي، كإلحاق التزوير المعلوماتي بباب تزوير المحررات، والاعتداء على المعطيات بجرائم الإتلاف.[2]

الفرع الثاني: الركن المادي

يتخذ الركن المادي في الجريمة الإلكترونية صورتين رئيسيتين: تتمثل الأولى في الاعتداء على أنظمة المعالجة الآلية للمعطيات، وتتجلى الثانية في الاعتداء على منتجات الإعلام الآلي وتحديداً عبر التزوير المعلوماتي.

بخصوص الصورة الأولى، فقد نصت المادة 394 مكرر من قانون العقوبات الجزائري على تجريم فعل الدخول والبقاء غير المشروعين في النظام، مقرة عقوبة الحبس من 6 أشهر السنتين وغرامة مالية. وتتخذ هذه الجريمة شكلاً بسيطاً يقتصر على مجرد الدخول أو البقاء عن طريق الغش، وشكلاً مشدداً تضاعف فيه العقوبة إذا اقترن الفعل بحذف أو تغيير لمعطيات المنظومة. وترتفع العقوبة إلى الحبس من سنةإلى 4سنوات إذا ترتب على ذلك تخريب نظام اشتغال المنظومة. وتُكيف جريمة الدخول غير المصرح به في التشريع الجزائري على أنها جريمة شكلية تتحقق بمجرد الوصول إلى المعلومات المخزنة بأي طريقة كانت، دون اشتراط تحقق نتيجة إجرامية معينة. [3]ويتلازم فعل الدخول غالباً مع فعل "البقاء"

1 علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، لبنان، 1999، ص 35.

2 مرجع نفسه ، ص24.

3 آمال قارة، الحماية الجزائية للمعلومات في التشريع الجزائري، الطبعة 2، دار هومة، الجزائر، 2007، ص 100.

غير المشروع، والذي أورده المشرع الجزائري على غرار الفقرة الأولى من المادة 323 من قانون العقوبات الفرنسي.[1]

ورغم هذا التفصيل، يُلاحظ أن المشرع الجزائري لم يورد نصاً مستقلاً يعاقب على "الاعتداء العمدي على سير النظام" بحد ذاته، بل اكتفى بتجريم الاعتداء العمدي على "المعطيات"، متبنياً تفسيراً ضمنياً مفاده أن الاعتداء على المعطيات يؤثر حتماً على صلاحية ووظائف النظام. [2]وهذا يطرح إشكالية إفلات بعض السلوكيات من العقاب إذا اقتصرت على عرقلة أو تعطيل أداء النظام العادي دون المساس بالمعطيات، لا سيما إذا كان الدخول أولياً مشروعاً .[3]أما بخصوص الاعتداء العمدي على المعطيات ذاتها، فقد حسمته المادة 394 مكرر 2 بعقوبات تصل إلى الحبس لخمس سنوات، مجرمةً أفعال التصميم، البحث، التجميع، التوفير، النشر، والاتجار في معطيات يمكن أن تُرتكب بها جرائم معلوماتية، إضافة إلى تجريم حيازة أو إفشاء تلك المعطيات.

أما الصورة الثانية للركن المادي فتتمثل في التزوير المعلوماتي، والذي يُعد من أخطر صور الغش نظراً لدقة الحواسيب الآلية. وفي هذا الإطار، اقتدى المشرع الجزائري بنظيره الفرنسي في إخضاع التزوير المعلوماتي للقواعد العامة التقليدية للتزوير. غير أن التباين بين نصوص قانون العقوبات الجزائري والفرنسي يجعل من هذا الإخضاع قاصراً، مما يفرض ضرورة تدخل المشرع لإدراج نص خاص ومستقل يعالج التزوير المعلوماتي بدقة تتناسب مع طبيعته التقنية.[4]

الفرع الثالث: الركن المعنوي

تُعد الجرائم الإلكترونية جرائم عمدية بطبيعتها، ويختلف ركنها المعنوي باختلاف السلوك الإجرامي المرتكب. ففي جريمة الدخول والبقاء غير المشروع، يتطلب القصد الجنائي إحاطة الجاني علماً بكافة عناصر الجريمة، وإدراكه بأن فعله ينصب على نظام معالجة آلية بما يحويه من برامج ومعلومات محمية قانوناً. ويضاف إلى ذلك ضرورة توافر "نية الغش"، والتي تُستشف من خلال تعمد خرق الجهاز الرقابي

1 المرجع نفسه، ص 110.

2 المرجع نفسه ، ص 190.

3 المرجع نفسه ، ص 113.

4 المرجع نفسه ، ص 133-134. (يُشار إلى أن المشرع الفرنسي استحدث نصاً خاصاً بالتزوير المعلوماتي سنة 1988، ثم تراجع عنه في تعديل 1994 وألغاه ليخضعه لنصوص التزوير العامة التقليدية).

للدخول، أو من طبيعة العمليات التي يجريها الجاني للبقاء داخل النظام وهو يعلم أن تواجده غير مرخص به.

أما في جريمة الاعتداء على سير نظام المعالجة الآلية، فإن أفعال العرقلة والتعطيل تفترض قصداً جنائياً منبعثاً من طبيعة الأفعال ذاتها، وهو ما يميزها عن الاعتداء غير العمدي الذي قد يُشكل مجرد ظرف مشدد لجريمة الدخول غير المشروع. وفيما يخص الاعتداءات العمدية على المعطيات (كالإدخال والمحو والتعديل)، فيُشترط توافر القصد الجنائي العام (العلم والإرادة) مقترناً بنية الغش، دون أن يُشترط بالضرورة توافر نية الإضرار بالغير؛ إذ تكتمل أركان الجريمة بمجرد اتجاه الإرادة لإحداث التعديل أو المحو مع العلم بذلك، بغض النظر عن تحقق الضرر الفعلي في الواقع. ويمتد هذا الحكم ليشمل جرائم استخدام المعطيات كوسيلة لارتكاب جرائم أخرى (كالتصميم والتوفير)، حيث يُشترط تلازم القصد الجنائي العام مع القصد الخاص المتمثل صراحة في نية الغش والتحايل.[1]

المطلب الثاني: إشكالية الإثبات وحجية الأدلة الإلكترونية

تفرض الجرائم المرتبطة بالعملات الرقمية تحدياً جوهرياً أمام القضاء يتمثل في إشكالية الإثبات؛ فبينما تعتمد الجرائم التقليدية على أدلة مادية ملموسة، تقع الجرائم الرقمية في بيئة افتراضية لا تترك سوى آثار إلكترونية ونبضات كهرومغناطيسية. هذا التحول الجذري في طبيعة مسرح الجريمة استوجب ضرورة الاعتراف بـ "الدليل الإلكتروني" وتحديد حجيته القانونية كوسيلة لإقامة الحجة أمام القضاء، وهو ما سيتم تفصيله من خلال تحديد ماهية هذه الأدلة(فرع أول)، ثم بيان قوتها الثبوتية في التشريع (فرع ثاني).

الفرع الأول: الأدلة الرقمية

يُعرف الإثبات الإلكتروني بأنه إقامة الحجة أو الدليل أمام الجهات القضائية باستخدام وسائل إلكترونية أو بيانات رقمية مستخرجة من أنظمة المعالجة الآلية. وتتجسد هذه الأدلة في الوثائق والمحررات الإلكترونية التي يتم إنشاؤها، معالجتها، تخزينها، أو استرجاعها عبر وسائط تقنية. لتأطير هذه المحررات، تدخلت التشريعات الدولية، وفي طليعتها قانون "الأونسيترال" النموذجي، لضبط المفاهيم؛ حيث تنقسم هذه المحررات أساساً إلى محررات معدة للإثبات وأخرى غير معدة له.[2]

1آمال قارة، مرجع سابق ، ص 125.

2كحيل حياة، حجية الإثبات الإلكتروني، مجلة البحوث والدراسات القانونية والسياسية، جامعة البليدة ط 2، العدد التاسع، الجزائر، ص 241.

تُعد "الكتابة الإلكترونية" حجر الزاوية في الأدلة المعدة للإثبات، وهي تتخذ شكل حروف أو أرقام أو رموز تثبت على دعامة إلكترونية وتُعطي دلالة قابلة للإدراك ومقروءة عبر شاشات الحواسيب. غير أن هذه الكتابة أو "رسالة البيانات" لا تكتسب صفة "المحرر الإلكتروني" المكتمل الأركان إلا باقترانها بـ "التوقيع الإلكتروني". فالتوقيع الإلكتروني، سواء كان رقمياً يعتمد على خوارزميات التشفير أو بيومترياً، يمثل الإجراء التقني الذي يضمن تحديد هوية المُوقِّع ويعبر عن إرادته وقبوله بمضمون المحرر، حامياً إياه من أي تعديل أو تحريف لاحق [1]

ولكي يُحتج بهذا السند الإلكتروني قانونياً، تشترط النظم القانونية توافر ضوابط دقيقة تتمثل في: وجود كتابة إلكترونية مقروءة، توقيع إلكتروني موثق يمنح السند نفس حجية السند العرفي، ووجود "شهادة تصديق" تصدر عن جهة محايدة ومرخصة (مقدمو خدمات المصادقة) لإثبات نسبة التوقيع لصاحبه، فضلاً عن إمكانية الاحتفاظ بالسند واسترجاعه في شكله الأصلي وقت الحاجة. وفي المقابل، توجد أدلة إلكترونية غير معدة أصلاً للإثبات ولكنها تُتخذ كقرائن، مثل الدفاتر التجارية الإلكترونية، ورسائل البريد الإلكتروني التي تثير إشكاليات جمة حول تحديد هوية مرسلها لغياب التوثيق الرسمي فيها.[2]

الفرع الثاني: حجية الإثبات

أحدثت مفرزات تقنية المعلومات هزة في القواعد الكلاسيكية للإثبات التي كانت ترتكز حصرياً على الدعامة الورقية ذات المدلول المادي. واستجابة لهذا التحدي، سارعت التشريعات المقارنة لتقييم وتعديل نصوصها بتوجيه من قوانين "الأونسيترال" التي أقرت مبدأ القبول القانوني للتوقيع والمحرر الإلكتروني. وفي هذا السياق، واكب المشرع الجزائري هذا التطور من خلال تعديل القانون المدني، حيث نصت المادة 323 مكرر 1 صراحة على أنه: "يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها.[3]"

إن هذا التوجه التشريعي الجزائري يفك الارتباط التقليدي بين الكتابة والورق، ليوسع مفهوم الدعامة لتشمل أي وسيط إلكتروني (كالأقراص والخوادم) شريطة أن تكون محتويات الكتابة مفهومة وقابلة للإدراك

1 كحيل حياة، المرجع نفسه، ص 242-244.

2 المرجع نفسه، ص 245-246.

3 المادة 323 مكرر 1 من الأمر رقم 75-58 المؤرخ في 26 سبتمبر 1975 المتضمن القانون المدني، المعدل والمتمم بالقانون رقم 05-10 المؤرخ في 20 يونيو 2005، الجريدة الرسمية للجمهورية الجزائرية، العدد 44. وكذا: كحيل حياة، المرجع السابق.

البشري وليست مجرد شفرات حاسوبية مبهمة. وقد تعزز هذا الاعتراف بتنظيم التوقيع الإلكتروني في المادة 327 (الفقرة 2) من القانون المدني الجزائري، والتي اعتدت بحجيته متى استوفى شروط السلامة وتحديد الهوية. وهذا يعني أن المشرع ساوى تماماً في القوة الثبوتية بين المحرر الإلكتروني الموثق والمحرر الورقي العرفي، جاعلاً من قواعد الإثبات قواعد متعلقة بالنظام العام لا يجوز مخالفتها.[1]

ومع ذلك، تتباين الحجية القانونية باختلاف قوة الدليل التقني. ففي حين يتمتع المستند الذكي المذيل بتوقيع إلكتروني مشفر ومصادق عليه بحجية قاطعة تعادل الدليل الكتابي، تبقى بعض الوسائل الأخرى، كرسائل البريد الإلكتروني، مفتقرة للثقة المطلقة في هوية مرسلها وسلامة محتواها من الاختراق. وعليه، فإن حجية هذه الرسائل تبقى نسبية وغير ملزمة بحد ذاتها، وتخضع تماماً للسلطة التقديرية لقاضي الموضوع، الذي يملك صلاحية الأخذ بها أو استبعادها بناءً على مدى اقتناعه بسلامتها التقنية وخلوها من التحريف، مما يعكس مرونة القضاء في التعامل مع الأدلة الرقمية غير الموثقة.[2]

المطلب الثالث: الإختصاص القضائي في جرائم العملات الرقمية

تُشكل مسألة الإختصاص القضائي العثرة الأبرز في الملاحقات الجزائية المرتبطة بالجرائم المعلوماتية عموماً، وجرائم العملات الرقمية على وجه الخصوص. فالقانون الجنائي التقليدي بُني هندسياً على ركيزة "الحدود الجغرافية" ومبدأ السيادة الإقليمية للدولة، في حين أن العملات المشفرة تتداول في فضاء سيبراني لامادي (Cyberspace) لا يعترف بالحدود، ويعتمد على شبكات لامركزية (سلاسل الكتل) تتوزع خوادمها في قارات مختلفة. هذا التناقض الصارخ بين مادية القاعدة القانونية وافتراضية مسرح الجريمة، أفرز إشكاليات معقدة حول تنازع الاختصاص الإيجابي والسلبي بين الدول، ودفع بالفقه والمشرع إلى إعادة تكييف قواعد (الاختصاص الوطني) و(الدولي) لاستيعاب هذه الظاهرة، وهو ما سنفصله في الفرعين الآتيين.

الفرع الأول: الإختصاص الوطني وإشكالية تكييف مبدأ الإقليمية

ينعقد الإختصاص الوطني كقاعدة عامة بناءً على مبدأ "إقليمية النص الجنائي"؛ حيث تبسط الدولة ولايتها القضائية على كل جريمة تقع داخل حدودها الإقليمية، بغض النظر عن جنسية فاعلها. غير أن تطبيق هذا المبدأ الكلاسيكي على جرائم العملات الرقمية يصطدم بعقبة تحديد "مكان ارتكاب الجريمة "

1 المادة 327 من القانون المدني الجزائري المعدل والمتمم..

2 كحيل حياة، المرجع نفسه، ص 250-252.

.(Locus Delicti)ففي جرائم الاحتيال الرقمي أو التداول غير المشروع، قد يتحقق الركن المادي (السلوك) في دولة معينة عبر النقر على لوحة المفاتيح، بينما تتحقق النتيجة الإجرامية (انتقال العملات المشفرة) في دولة أخرى، وتمر البيانات عبر خوادم دولة ثالثة.

وأمام هذا التشتت المادي، انقسم الفقه الجنائي في تحديد معيار الإقليمية إلى نظريتين: "نظرية السلوك الإجرامي" التي تعقد الاختصاص لمحاكم الدولة التي تم فيها تنفيذ الفعل (كإرسال الفيروس أو إعطاء أمر التحويل)، و"نظرية النتيجة" التي تمنح الاختصاص لمحاكم الدولة التي تحقق فيها الضرر (كمكان تواجد حساب الضحية). وقد مالت معظم التشريعات الجنائية الحديثة إلى الأخذ بالمعيار المزدوج، حيث يكفي أن يقع أي عمل من أعمال البدء في التنفيذ، أو تتحقق النتيجة الإجرامية، أو حتى جزء منها داخل إقليم الدولة، لينعقد الاختصاص لمحاكمها الوطنية.[1]

أما على المستوى المؤسسي والتنظيمي، فقد أدركت التشريعات العربية أن المحاكم العادية بتركيبتها التقليدية تقف عاجزة أمام التعقيد التقني لجرائم العملات الرقمية، مما استوجب خلق آليات قضائية ذات اختصاص محلي موسع. وفي هذا السياق، يعتبر المشرع الجزائري رائداً من خلال استحداثه "للأقطاب الجزائية المتخصصة". وتتويجاً لهذا المسار، وبموجب الأمر رقم 21-11 المتمم لقانون الإجراءات الجزائية، تم إنشاء "القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال" على مستوى محكمة مقر مجلس قضاء الجزائر.[2]

وقد خرج المشرع الجزائري بهذا القطب عن القواعد العامة للاختصاص المحلي، حيث نصت المادة 211 مكرر 23 صراحة على أن وكيل الجمهورية وقاضي التحقيق ورئيس هذا القطب يمارسون صلاحياتهم "في كامل الإقليم الوطني". ويختص هذا القطب حصرياً بالمتابعة والتحقيق في جرائم المساس بأنظمة المعالجة الآلية للمعطيات والجرائم ذات الطابع المنظم أو العابر للحدود. ويمثل هذا التمديد الاستثنائي للاختصاص الإقليمي ضمانة جوهرية لتوحيد الاجتهاد القضائي، وتجاوز عقبة تنازع

1 محمود نجيب حسني، شرح قانون العقوبات القسم العام، الطبعة السادسة، دار النهضة العربية، القاهرة، 1989، ص 154.

2 ليندة بومحراث، "الأقطاب الجزائية المتخصصة كآلية لمكافحة الجرائم الإلكترونية"، مداخلة مقدمة في الملتقى الدولي: التكنولوجيات الحديثة والجريمة، كلية الحقوق، جامعة الإخوة منتوري قسنطينة 1، الجزائر، 13 نوفمبر 2022، ص 6-9.

الاختصاص بين المحاكم المحلية، فضلاً عن توفير كادر قضائي متمرس تقنياً قادر على استيعاب تعقيدات البلوك تشين وتتبع مسارات العملات الرقمية.[1]

وفي مقاربات عربية أخرى، ربطت بعض الدول ذات التوجه التنظيمي (كالإمارات والبحرين) اختصاصها الوطني في جرائم الأصول الافتراضية بمعيار "الاستهداف" أو "مقر تقديم الخدمة". فمتى كان مزود خدمات الأصول الافتراضية (VASP) موجهاً نشاطه نحو الجمهور داخل الدولة، أو كان يتخذ منها مقراً قانونياً له، انعقد الاختصاص لمحاكمها الوطنية لملاحقته بتهم مزاولة نشاط مالي دون ترخيص أو مخالفة لوائح مكافحة غسل الأموال، حتى وإن كانت الخوادم الفعلية للمنصة تقع خارج الحدود الإقليمية.[2]

الفرع الثاني: الاختصاص الدولي وآليات التعاون العابر للحدود

نظراً لكون جرائم العملات الرقمية جرائم "عابرة للحدود" بطبيعتها، فإن مبدأ الإقليمية يقف قاصراً إذا وقعت الجريمة بالكامل خارج حدود الدولة المستهدفة. لتدارك هذا الفراغ التشريعي وتفادي تحول بعض الدول إلى "ملذات آمنة" للقراصنة ومبيضي الأموال، تلجأ الأنظمة القانونية إلى تفعيل مبادئ الاختصاص الاحتياطية ذات الامتداد الدولي، والتي تستند إلى روابط شخصية أو موضوعية تبرر تدخل القاضي الوطني.

يتجسد الامتداد الأول في "مبدأ الشخصية"، بشقيه الإيجابي والسلبي. إذ يقر الفقه الجنائي الدولي بصلاحية المحاكم الوطنية في محاكمة الجاني الذي يحمل جنسية الدولة متى ارتكب جريمة رقمية في الخارج وعاد إلى وطنه (الشخصية الإيجابية)، وذلك تكريساً لمبدأ "لا تسليم للمواطنين". كما يعقد الاختصاص استناداً لجنسية المجني عليه (الشخصية السلبية)، حيث تتدخل الدولة الجزائرية لحماية ذمة مواطنيها المالية من عمليات الاحتيال الرقمي وسرقة المحافظ المشفرة حتى لو تم اختراقها من طرف أجانب متواجدين في قارات أخرى. أما الامتداد الثاني والأخطر فيتمثل في "مبدأ العينية أو الحماية"؛ والذي يمنح القضاء الوطني ولاية عالمية لملاحقة أي شخص، أياً كانت جنسيته، وفي أي مكان ارتكب

1 ليندة بومحراث، مرجع سبق ذكره ، ص 14-17. (بالاستناد إلى المواد 211 مكرر 22 و 211 مكرر 23 من الأمر 21-11 المتمم لقانون الإجراءات الجزائية).

2 قوانين وأنظمة تنظيم الأصول الافتراضية المقارنة (كالتشريع الإماراتي والبحريني).

فيه جريمته، متى كان الفعل يشكل استهدافاً مباشراً للمصالح الأساسية للدولة، مثل عمليات غسل الأموال الضخمة عبر البيتكوين التي تهدف إلى ضرب الاقتصاد الوطني، أو تمويل الإرهاب لزعزعة أمن الدولة.[1]

ورغم قوة هذه المبادئ النظرية في إرساء الاختصاص الدولي، إلا أن تفعيلها الإجرائي يصطدم بعقبات تطبيقية قاهرة. فتنفيذ أوامر القبض الدولية، وتجميد المحافظ الرقمية الموجودة في الخارج، وجمع الأدلة (الإلكترونية) كعناوين IP و(سجلات البلوك تشين)يتطلب بالضرورة الخضوع لمبدأ سيادة الدول الأخرى. من هنا، أضحت الاتفاقيات الدولية ضرورة حتمية وليست خياراً. وتبرز اتفاقية مجلس أوروبا المتعلقة بالجرائم المعلوماتية (اتفاقية بودابست لسنة 2001) كأهم إطار قانوني دولي يهدف إلى حل إشكالية تنازع الاختصاص عبر مادتها الـ 22، حيث تُلزم الدول الأعضاء بتأسيس قواعد اختصاصها، وتضع آليات سريعة لحسم التنازع الإيجابي متى ادعت أكثر من دولة اختصاصها بالنظر في ذات الجريمة الرقمية، مفضلة معيار الدولة الأكثر ارتباطاً بالجريمة أو التي يتواجد فيها الجاني مادياً لضمان فعالية المحاكمة.[2]

وعلاوة على ذلك، يقتضي الاختصاص الدولي تفعيل آليات المساعدة القضائية المتبادلة (MLATs)والإنابات القضائية الدولية بشكل فوري. ففي عالم التشفير، يتطلب تتبع الأموال سرعة فائقة قبل أن يتم تمريرها عبر "خلاطات العملات (Mixers) "التي تطمس مسارها. لذا، تعمل التوصيات الدولية، لاسيما توصيات مجموعة العمل المالي (FATF) ، على حث الدول لسد الفجوات القضائية وتسهيل تبادل الأدلة الرقمية وتسليم المجرمين، لضمان أن الفضاء الافتراضي لا يشكل حصانة قضائية لمرتكبي الجرائم المالية.[3]

نستنتج من دراسة هذا المبحث أن تطبيق القواعد العامة للمسؤولية الجنائية على جرائم العملات الرقمية يواجه صعوبات عملية وقانونية. فبالرغم من محاولات المشرع تكييف هذه الأفعال ضمن نصوص "المساس بأنظمة المعالجة الآلية للمعطيات"، تظل عملية الإثبات معقدة بسبب الطبيعة المشفرة واللامادية للأدلة. وإلى جانب ذلك، أظهرت قواعد الاختصاص القضائي التقليدية قصوراً واضحاً أمام جرائم لا

1 عبد الفتاح بيومي حجازي، الاختصاص القضائي في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية، 2007، ص 85 وما بعدها.

2 المادة 22 من اتفاقية بودابست المتعلقة بالجرائم المعلوماتية (Convention on Cybercrime)، مجلس أوروبا، 2001.

3 مبادئ وتوصيات مجموعة العمل المالي (FATF) الخاصة بمخاطر الأصول الافتراضية، التقرير التوجيهي، 2020.

تعترف بالحدود الجغرافية، مما استدعى توسيع الاختصاص المحلي بإنشاء أقطاب جزائية متخصصة، والاعتماد على مبادئ الاختصاص الدولي والتعاون القضائي لضمان ملاحقة الجناة.

خلاصة الفصل:

أظهرت الدراسة في هذا الفصل أن العملات الرقمية فرضت نفسها كواقع مالي وتقني جديد يتجاوز كونه مجرد ابتكار عابر. وتتسم هذه العملات بطبيعة مزدوجة؛ فبينما تقدم حلولاً سريعة ومبتكرة للتحويلات المالية، فإنها تخلق في الوقت نفسه بيئة ملائمة لتطور الجريمة، مستفيدة من غياب الرقابة المركزية وطبيعتها المشفرة .وقد أبانت المعالجة القانونية عن وجود تحديات حقيقية تواجه أجهزة إنفاذ القانون، لاسيما في استخراج الأدلة الرقمية والاعتداد بها، وفي تحديد الجهة القضائية المختصة بمتابعة جرائم تتجاوز الحدود الإقليمية. وهذا التأسيس النظري والقانوني يضعنا مباشرة أمام ضرورة البحث في التطبيقات العملية، وهو ما سنفصله في الفصل الثاني من خلال دراسة صور الجرائم المرتبطة بالعملات الرقمية والآليات القانونية لمكافحتها.

الفصل الثاني: الجرائم المرتبطة بالعملات الرقمية وآليات مكافحتها

الفصل الثاني: الجرائم المرتبطة بالعملات الرقمية وآليات مكافحتها

بعد أن أرسى الفصل الأول الدعائم النظرية والقانونية للعملات الرقمية، ننتقل في هذا الفصل إلى ملامسة الشق التطبيقي والواقع الإجرامي المتطور لهذه الأصول في الفضاء السيبراني. فقد أدى التحول الرقمي إلى انتقال النشاط الإجرامي نحو البيئة الإلكترونية، مستفيداً من الخصائص التي توفرها العملات المشفرة، لاسيما السرية، وإخفاء الهوية، وصعوبة تتبع العائدات غير المشروعة. وعليه، قسمنا هذا الفصل إلى مبحثين:

المبحث الأول: صور الجرائم المرتبطة بالعملات الرقمية.

المبحث الثاني: آليات مكافحة الجرائم المرتبطة بالعملات الرقمية.

المبحث الأول: صور جرائم العملات الرقمية

بعد الانتقال من الجانب المفاهيمي والقانوني إلى الجانب التطبيقي، يقتضي هذا المبحث الوقوف على أبرز الصور الإجرامية التي أفرزها استعمال العملات الرقمية في البيئة الرقمية. فقد ساهمت خصائص هذه العملات، كإخفاء الهوية وسرعة التحويل والطابع العابر للحدود، في تسهيل ارتكاب جرائم مالية وتقنية يصعب كشفها بالوسائل التقليدية. وعليه، قسمنا هذا المبحث إلى ثلاثة مطالب:

- **المطلب الأول: جرائم الاحتيال والاستغلال الوهمي.**
- **المطلب الثاني: جرائم غسل الأموال وتمويل الأنشطة غير المشروعة.**
- **المطلب الثالث: جرائم الاختراق وسرقة المحافظ الرقمية.**

المطلب الأول: جرائم الاحتيال والاستغلال الوهمي

في ظل التوسع المتسارع للتعاملات الرقمية، والانتشار المتزايد للعملات المشفرة في الأسواق المالية غير التقليدية، أصبحت جرائم الاحتيال المرتبطة بهذه الأصول تمثل أحد أخطر مظاهر الإجرام السيبراني الحديث. فهذه الجرائم لا تقوم فقط على استغلال جهل الضحايا أو طمعهم في تحقيق أرباح سريعة، بل تعتمد كذلك على توظيف تقنيات رقمية معقدة، وثغرات أمنية، وأساليب تضليل إلكتروني يصعب اكتشافها في مراحلها الأولى.

وتكمن خطورة هذا النوع من الجرائم في أن المحتالين يستغلون الطبيعة التقنية للعملات الرقمية، وما توفره من سرعة في التحويل وصعوبة نسبية في تتبع الهوية، للوصول إلى المحافظ الإلكترونية أو المعطيات الشخصية للمستخدمين، مما يؤدي إلى إلحاق خسائر مالية جسيمة بالمستثمرين. كما يعتمد هؤلاء الجناة بصورة متزايدة على تقنيات **الهندسة الاجتماعية**، ومواقع التواصل الاجتماعي، والمنصات الاستثمارية الوهمية، لاستدراج الضحايا وإقناعهم بالدخول في مشاريع لا وجود لها في الواقع.

ومن ثم، فإن دراسة جرائم الاحتيال والاستغلال الوهمي في مجال العملات الرقمية تقتضي بيان أهم الأساليب الإجرامية المستعملة في هذا المجال(فرع أول)، ثم التطرق إلى وسائل كشف هذه الجرائم وتتبعها، (فرع ثاني)، مع إبراز موقف التشريعات المقارنة والوطنية من مواجهتها(فرع ثالث).

الفرع الأول: أساليب الاحتيال في العملات الرقمية

تتطور الجريمة المرتبطة بالأصول المشفرة بصورة متسارعة، مستفيدة من الخصائص التقنية التي تميز هذا المجال، ولا سيما صعوبة تحديد هوية المتعاملين، والطابع اللامركزي لبعض العمليات، وسرعة انتقال القيم الرقمية عبر الحدود. وتعتمد هذه الجرائم أساساً على تقنية سلسلة الكتل (**Blockchain**)، التي يُطلق عليها في بعض الكتابات القانونية اسم **"جهاز التسجيل الإلكتروني المشترك**[1]**."**

ورغم أن هذه التقنية تُعد من أهم الابتكارات الرقمية المعاصرة، لما توفره من شفافية تقنية وإمكانية لتسجيل المعاملات بطريقة موزعة، إلا أن استعمالها في مجال العملات الرقمية أثار مخاوف قانونية وأمنية جدية. فقد أصبحت بعض العملات المشفرة توصف في الفقه بأنها **"عملات إجرامية"**، نتيجة افتقارها إلى معايير الثقة والائتمان البنكي التقليدي، وسهولة توظيفها في أنشطة غير مشروعة، مثل تبييض الأموال، والتهرب الضريبي، وتمويل المعاملات المحظورة.[2]

ومن أبرز صور الاحتيال في هذا المجال ما يُعرف بـ **الكريبتوجاكينغ(Cryptojacking)**أو التعدين السري. ويقصد به قيام الجاني باستغلال موارد جهاز الضحية دون علمه أو موافقته، بهدف تعدين العملات المشفرة. ويتم ذلك عادة عن طريق زرع برمجيات خبيثة (**Malware**)داخل النظام المعلوماتي، أو من خلال مواقع إلكترونية مصابة، أو روابط مضللة. وبمجرد تشغيل الجهاز أو الدخول إلى الموقع المصاب، تُستغل القدرة الحوسبية للضحية في حل المعادلات الرياضية اللازمة لعمليات التعدين.

وتزداد خطورة هذا الأسلوب عندما يتعلق الأمر بعملات رقمية توفر قدراً عالياً من الخصوصية، مثل (Monero)، لأنها تجعل تتبع مصدر الأموال والجهات المستفيدة منها أكثر صعوبة. ولا يقتصر أثر الكريبتوجاكينغ على الجانب المالي فقط، بل يمتد إلى إبطاء أداء الأجهزة، واستهلاك الطاقة، وتعريض الأنظمة المعلوماتية لمخاطر أمنية إضافية.[3]

1G. MARRAUD des GROTTES, Auditions au Sénat sur la blockchain : les incompréhensions demeurent..., RLDA N°135, 1er mars 2018.

2ALUMASEANU S., Le traitement pénal du Bitcoin et des autres monnaies virtuelles, Gaz. Pal 2014, no 242.

3 أكاديمية البيتكوين العربية، "ما هو كريبتوجاكينج Cryptojacking؟"، موقع أكاديمية البيتكوين العربية، منشور بتاريخ 08 مارس 2023، متاح على الرابط: https://btcacademy.online/ما-هو-كريبتوجاكينج-cryptojacking؟/،

وإلى جانب التعدين السري، تبرز جرائم **احتيال عروض العملات الأولية(ICOScams)**باعتبارها من أكثر الأساليب شيوعاً في مجال الاستثمار الوهمي. فالطرح الأولي للعملة يُستعمل في الأصل كوسيلة لتمويل الشركات الناشئة والمشاريع الرقمية، من خلال بيع عملات أو رموز رقمية للمستثمرين قبل إطلاق المشروع. غير أن المحتالين يستغلون هذه الآلية لتسويق مشاريع وهمية، فيقدمون وعوداً بعوائد مرتفعة ونمو سريع، مدعومة بوثائق بيضاء (**Whitepapers**)مزيفة، ومعلومات غير صحيحة عن فريق العمل أو التكنولوجيا المستعملة.

وفي هذه الحالة، يُدفع المستثمرون إلى تحويل أموالهم بناءً على تصورات مضللة، ثم يختفي القائمون على المشروع بمجرد جمع المبالغ المطلوبة، دون تنفيذ المشروع أو إعادة الأموال. [1] وتزداد خطورة هذه الجرائم بالنظر إلى أن عدداً من البنوك المركزية، مثل البنك المركزي الأوروبي وبنك فرنسا، لا تعترف بالبيتكوين وغيرها من الأصول المشفرة كعملة حقيقية، لافتقارها إلى خصائص وسيلة الدفع المستقرة واحتياطي القيمة، وهو ما يجعل الاستثمار فيها محفوفاً بدرجة عالية من المخاطر.[2]

كما شهد مجال العملات الرقمية عودة لصور احتيالية كلاسيكية، ولكن في قالب رقمي حديث، وعلى رأسها **مخططات بونزي(Ponzi Schemes)** .وتقوم هذه المخططات على وعد المستثمرين بعوائد مرتفعة وغير واقعية، مع دفع أرباح للمستثمرين القدامى من أموال المستثمرين الجدد، وليس من نشاط اقتصادي حقيقي. وتستمر هذه المنظومة طالما استمر تدفق الأموال الجديدة، لكنها تنهار بمجرد تراجع عدد المنضمين أو مطالبة عدد كبير من المستثمرين بسحب أموالهم.[3]

وتتقاطع هذه المخططات مع إنشاء مواقع استثمار مزيفة، تشبه في شكلها منصات التداول أو سوق صرف العملات الأجنبية(**Forex**)، حيث يتم إيهام الضحايا بوجود فرص استثمارية مربحة في أصول

تاريخ الولوج: 14 ماي 2026، الساعة: 10:30.

1 أكاديمية البيتكوين العربية، "احتيال عروض العملات الأولية ICO Scam"، موقع أكاديمية البيتكوين العربية، دون تاريخ نشر، تاريخ الولوج: 14 ماي 2026، الساعة: 10:30.

2 منصة Rain، "ما هو ICO؟ العرض الأولي للعملة"، موقع Rain، منشور بتاريخ 05 نوفمبر 2025، متاح على الرابط: https://www.rain.com/ar/learn/what-is-an-ico، تاريخ الولوج: 14 ماي 2026، الساعة: 10:30

3 موقع Cryptopolitan، "مخططات بونزي مقابل الهرم: احذر من الخداع"، موقع Cryptopolitan، متاح على الرابط: https://www.cryptopolitan.com/ar/ponzi-scheme-vs-pyramid-scheme/، تاريخ الولوج: 14 ماي 2026، الساعة: 10:30.

رقمية أو محافظ تداول وهمية. غير أن هذه المنصات لا تهدف في الواقع إلى إدارة استثمارات حقيقية، بل إلى جمع أموال الضحايا ثم الامتناع عن ردها أو إغلاق الموقع نهائياً.

ولا تقتصر خطورة العملات المشفرة على جرائم الاحتيال الاستثماري، بل تمتد إلى استخدامها كوسيلة دفع في أنشطة إجرامية منظمة. فقد أصبحت الأصول المشفرة وسيلة مفضلة لمشغلي **الشبكة المظلمة** (**Darknet**)، وعصابات الاتجار بالمخدرات، ومطلقي برامج الفدية الخبيثة(**Ransomware**)، لما توفره من قدرة على إخفاء الهوية والابتعاد عن الرقابة التقليدية للنظام المالي والمصرفي. ويسهل ذلك إخفاء عائدات الجرائم، وتدوير الأموال غير المشروعة، والتهرب من آليات الرقابة الضريبية والمالية.[1]

ومن التطبيقات العملية الدالة على هذه الخطورة قضية منصة(**BTC-e**)، حيث تم توقيف مؤسسها سنة 2017 للاشتباه في تورطه في تبييض ما يقارب **9.4مليون بيتكوين** عبر المنصة. وقد أُدين لاحقاً في فرنسا بعقوبة الحبس بعد ثبوت تورطه في غسل الأموال ضمن عصابة منظمة، وهو ما يكشف أن منصات التداول غير المنظمة قد تتحول إلى أدوات مركزية في شبكات الإجرام المالي الرقمي.[2]

الفرع الثاني: وسائل كشف وتتبع جرائم الاحتيال الرقمي والمواجهة التشريعية

أمام اتساع نطاق الجرائم المرتبطة بالعملات الرقمية، سارعت عدة تشريعات وطنية وأنظمة دولية إلى البحث عن آليات تسمح بكشف المعاملات المشبوهة، وتتبع التدفقات المالية، وربط العمليات الرقمية بهويات حقيقية قدر الإمكان. فالهدف الأساسي من هذه الآليات هو كسر حاجز إخفاء الهوية الذي يشكل أحد أهم عناصر الجاذبية الإجرامية للأصول المشفرة.

وفي الجزائر، اتسم موقف المشرع بدرجة واضحة من الصرامة منذ مرحلة مبكرة، حيث تدخل بموجب قانون المالية لسنة 2018، وبالأخص المادة 117 منه، ليحظر شراء العملة الافتراضية أو بيعها أو استعمالها أو حيازتها. وقد برر هذا التوجه بكون العملة الافتراضية تفتقر إلى الدعامة المادية ولا تصدر عن جهة رسمية، مما يجعلها خارجة عن النظام النقدي المعترف به.

---

1 وزارة الاقتصاد والمالية والإنعاش الفرنسية، وحدة معالجة المعلومات والعمل ضد الدوائر المالية السرية TRACFIN، تقرير الاتجاهات وتحليل مخاطر غسل الأموال وتمويل الإرهاب 2019-2020، باريس، 2020، متاح على موقع وزارة الاقتصاد والمالية الفرنسية، تاريخ الولوج: 14 ماي 2026، الساعة: 10:30.

2CNN بالعربية، "اليونان تُسلم أمريكا مواطناً روسياً متهماً بتبييض الأموال"، 04 أوت 2022، تاريخ الولوج: 14 ماي 2026، الساعة: 10:30.

غير أن هذا الحظر الصريح لم يرافقه تحديد دقيق لطبيعة العقوبة المقررة عند مخالفة النص، الأمر الذي يطرح إشكالاً عملياً أمام القضاء. ففي غياب نص عقابي خاص ومفصل، قد يضطر القاضي إلى الرجوع إلى القواعد العامة، وخاصة جريمة **النصب والاحتيال** المنصوص عليها في المادة 372 من قانون العقوبات، متى توافرت عناصرها من استعمال طرق احتيالية، وإيهام الضحية، والاستيلاء على أموالها.

كما أن صدور القانون النقدي والمصرفي رقم 09-23 لم يحسم وضعية العملات المشفرة المستقلة بصورة شاملة، إذ اقتصرت المادتان 59 و74 على تنظيم وسائل الدفع الإلكترونية، ومنها الدينار الرقمي، دون أن يضع المشرع نظاماً قانونياً خاصاً بتتبع العملات المشفرة اللامركزية أو تنظيم منصات تداولها.

ولسد جزء من هذه الثغرة، اتجه المشرع الجزائري إلى توظيف قوانين الوقاية من تبييض الأموال وتمويل الإرهاب من أجل ملاحقة التدفقات المالية المشبوهة المرتبطة بالأصول الرقمية. ففي سنة 2012، تم توسيع مفهوم الأموال ليشمل القيم المالية الافتراضية والممتلكات غير المادية. [1] ثم تأكد هذا التوجه بصورة أوضح بموجب التعديل الصادر سنة 2023، حيث أُدرجت **الأصول الافتراضية** صراحة ضمن القيم الرقمية القابلة للتداول.[2]

وبناءً على توجيهات مجموعة العمل المالي (**FATF**)، أصبحت المؤسسات المالية والمصرفية مطالبة بتفعيل آليات الإخطار بالشبهة عند رصد عمليات مالية غير عادية أو مرتبطة بأصول رقمية مشبوهة. وتؤدي هيئات مثل خلية الاستعلام المالي (**CTRF**) وبنك الجزائر دوراً مهماً في تتبع التدفقات المشبوهة، وتحليل المعلومات المالية، وإحالة الملفات عند الاقتضاء إلى الجهات المختصة.

أما في القانون المقارن، فقد اختارت فرنسا مساراً تنظيمياً أكثر تفصيلاً، إذ أخضعت الأصول المشفرة لتكييف قانوني ضمن قانون **الميثاق(PACTE)** لسنة 2019، والمادة **L54-10-1**من تقنين النقد والمالية، بما سمح بإدراج هذه الأصول ضمن إطار قانوني أكثر وضوحاً من حيث التعريف والرقابة وتنظيم مزودي الخدمات.[3]

---

1 الأمر رقم 12-02 المؤرخ في 13 فبراير 2012، المعدل والمتمم للقانون رقم 05-01 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، الجريدة الرسمية، العدد 8، 2012

2 المادة 04 من القانون رقم 23-01 المؤرخ في 07 فبراير 2023، المعدل والمتمم للقانون 06-05، الجريدة الرسمية، العدد 08، 2023.

3Mathis B., Quel régime juridique pour les cryptoactifs, RLDA 2018/143, Suppl., n° 6613.

وعلى المستوى الأوروبي، تم اعتماد لائحة **أسواق الأصول المشفرة(MiCA)**، التي يُنتظر دخولها حيز التنفيذ أواخر سنة 2024، بهدف وضع إطار تنظيمي موحد وشفاف للأصول المشفرة داخل الاتحاد الأوروبي. وتأتي هذه اللائحة في سياق الحاجة إلى حماية المستثمرين، وتعزيز الشفافية، ومواجهة الانهيارات والاحتيالات التي عرفها سوق العملات المشفرة، فضلاً عن تمكين السلطات من تتبع المحتالين ومراقبة مزودي خدمات الأصول الرقمية.[1]

أما في الولايات المتحدة الأمريكية، فتتوزع مهام الرقابة والتتبع بين عدة جهات. فتتولى هيئة الأوراق المالية والبورصات (**SEC**)مراقبة عروض العملات الأولية (**ICOs**)متى اعتُبرت أوراقاً مالية، وذلك لحماية المستثمرين من الاحتيال والتضليل. كما تُلزم شبكة مكافحة الجرائم المالية (**FinCEN**)منصات التداول ومزودي الخدمات بمتطلبات الإبلاغ والامتثال، من أجل تتبع عمليات غسل الأموال والتمويل غير المشروع.

وعلى مستوى الولايات، تبرز ولاية نيويورك بنظام (**BitLicense**)، الذي يُعد من الأنظمة الصارمة في تنظيم مزودي خدمات العملات الافتراضية. وفي المقابل، تسعى ولايات أخرى، مثل كاليفورنيا وتكساس، إلى تحقيق توازن بين تشجيع الابتكار التكنولوجي وضبط المعاملات للوقاية من الاحتيال المالي.[2]

وبناءً على ما سبق، يتضح أن مواجهة جرائم الاحتيال والاستغلال الوهمي في العملات الرقمية لا يمكن أن تعتمد على الحظر وحده، ولا على التنظيم وحده، بل تحتاج إلى منظومة متكاملة تجمع بين التجريم، والرقابة المالية، والإخطار بالشبهة، وتنظيم مزودي الخدمات، والتعاون الدولي. فالرهان الحقيقي يكمن في تقليص مساحة إخفاء الهوية التي يستغلها الجناة، مع الحفاظ في الوقت نفسه على قدرة القانون على مواكبة التطور التقني السريع لهذا المجال.

1 لائحة الأسواق في الأصول المشفرة الأوروبية MiCA – Markets in Crypto-Assets.

2 أديتيا نارين ومارينا موريتي، تنظيم العملات المشفرة، مجلة التمويل والتنمية، صندوق النقد الدولي، سبتمبر 2022 ص 80.

المطلب الثاني: جرائم تبييض الأموال وتمويل الأنشطة غير المشروعة باستخدام العملات الرقمية

يُعد الاستقرار المالي والاقتصادي أحد المرتكزات الأساسية لضمان سيادة الدولة واستمرارية مؤسساتها. غير أن جرائم غسل الأموال وتمويل الأنشطة غير المشروعة تمثل تهديداً مباشراً لهذا الاستقرار، خاصة بعد انتقالها من الأساليب التقليدية إلى أنماط رقمية مستحدثة أكثر تعقيداً وصعوبة في الكشف.

وقد وفّرت العملات الرقمية المشفرة، بفعل طبيعتها اللامركزية وما تمنحه من سرعة في التحويل وقدر من السرية، بيئة ملائمة لعصابات الجريمة المنظمة لإخفاء العائدات غير المشروعة وإضفاء مظهر الشرعية عليها. فالخطر لم يعد مقتصراً على تداول أموال مجهولة المصدر داخل النظام المالي التقليدي، بل أصبح يمتد إلى فضاء رقمي عابر للحدود، يصعب ضبطه بالوسائل الرقابية الكلاسيكية.

ومن هذا المنطلق، يقتضي تناول هذا المطلب بيان **آليات غسل الأموال عبر العملات الرقمية** في (الفرع الأول)، ثم إبراز **طرق تتبع الأموال المشبوهة ودور الجهات الرقابية** في (الفرع الثاني).

الفرع الأول: آليات غسل الأموال عبر العملات الرقمية

يعتمد مبيضو الأموال في البيئة الرقمية على الجمع بين الأساليب الإجرامية التقليدية والتكنولوجيا المالية الحديثة، بهدف تحقيق السرعة في نقل الأموال، وإخفاء هوية المتعاملين، وتجنب الرقابة المصرفية والجمركية. وتظهر هذه الآليات في صور متعددة، تختلف من حيث الوسيلة، لكنها تتفق في الهدف، وهو إخفاء المصدر غير المشروع للأموال وإعادة إدماجها في الدورة الاقتصادية بصورة تبدو مشروعة.

أولاً: الشركات الوهمية كواجهة لإضفاء المشروعية

تُعد الشركات الوهمية من أبرز الآليات المستعملة في غسل الأموال عبر العملات الرقمية. وهي كيانات تُنشأ من الناحية القانونية دون أن تمارس نشاطاً اقتصادياً فعلياً، ويكون الهدف منها استغلال ذمتها المالية واسمها التجاري لفتح حسابات مصرفية تستقبل العائدات المشفرة.[1]

وتسمح هذه الواجهات القانونية بإضفاء مظهر الشرعية على الأموال الملوثة، سواء من خلال تهريبها إلى الخارج، أو إعادة توجيهها نحو أنشطة غير مشروعة، مثل الاتجار بالخمور أو الدعارة أو

1 – أديتيا نارين ومارينا موريتي، مرجع سابق ، ص 81.

الميسر. كما قد تُستغل هذه الأموال في دول ذات اقتصادات هشة لإنشاء مشاريع تبدو في ظاهرها قانونية، بينما تكون في حقيقتها وسيلة لإخفاء المصدر الإجرامي للأموال.[1]

ثانياً: تحويل الأصول الرقمية إلى أصول مادية ثمينة

إلى جانب الشركات الوهمية، يلجأ غاسلو الأموال إلى تسييل ثرواتهم الرقمية عبر شراء أصول مادية مرتفعة القيمة، مثل المعادن النفيسة، والأحجار الكريمة، والعقارات. وتكمن أهمية هذه الوسيلة بالنسبة للجناة في أن هذه الأصول يسهل نقلها أو إخفاؤها أو إعادة بيعها، مما يُعقد عملية تتبع مصدر الأموال.

وتتم هذه العمليات غالباً باستخدام بطاقات دفع مرتبطة بمحافظ مشفرة، أو عبر منصات تسمح بمقايضة الأصول الرقمية بسلع عينية. وبعد ذلك، تدخل هذه السلع إلى البلد الأم تحت غطاء معاملات تجارية مشروعة، فيختفي المصدر الحقيقي للأموال داخل سلسلة من العمليات الظاهرية التي يصعب تفكيكها.[2]

ثالثاً: الارتباط بجرائم المخدرات والتهريب المالي

تتقاطع آليات غسل الأموال عبر العملات الرقمية بشكل وثيق مع جرائم الاتجار بالمخدرات والمؤثرات العقلية، وهي جرائم تُلحق أضراراً نفسية وجسدية جسيمة بالأفراد، وتمس في الوقت نفسه بالنسيج الاقتصادي والاجتماعي للدولة. فالعائدات الضخمة التي تنتج عن هذه الجرائم خلال فترات قصيرة تحتاج إلى وسائل سريعة وآمنة لإخفائها، وهو ما توفره العملات الرقمية بسبب صعوبة تتبعها وسرعة تحويلها.

وبعد تحويل هذه العائدات عبر الأصول الرقمية، يُعاد ضخها في قنوات رسمية، لتظهر وكأنها أرباح ناتجة عن أنشطة تجارية قانونية، في حين أنها في حقيقتها أموال متأتية من نشاط إجرامي.[3]

ويترافق ذلك مع نشاط التهريب المالي، حيث تُنقل القيم المالية المشفرة من دولة إلى أخرى في وقت قصير، بعيداً عن الالتزامات القانونية والجمركية التي تفرضها القنوات المالية التقليدية. وتساعد الطبيعة

---

1 حمد سفر، مكافحة غسل الأموال في البلدان العربية، بيروت: اتحاد المصارف العربية، 2003، ص. 124.

2 لعشب علي، الإطار القانوني لمكافحة تبييض الأموال، ط. 2، الجزائر: ديوان المطبوعات الجامعية، 2009، ص. 32.

3 المادة 2 من القانون رقم 23-05 المؤرخ في 7 مايو 2023، المتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والاتجار غير المشروعين بها، الجريدة الرسمية للجمهورية الجزائرية، العدد 32، الصادرة في 9 مايو 2023.

اللامركزية لهذه الأصول في التجهيل بمصدرها، مما يفتح المجال أمام الجناة لإخفاء الأموال وتجاوز الرقابة.[1]

رابعاً: أنظمة الدفع الإلكترونية وإعادة إدماج الأموال

تلعب أنظمة الدفع الإلكترونية دوراً مهماً في تسهيل عمليات غسل الأموال، إذ يتم إيداع مبالغ مالية رقمية لدى بنوك أجنبية، ثم تُسحب لاحقاً في البلد الأم عن طريق بطاقات الائتمان. وتسمح هذه الطريقة للمجرمين بتجنب حيازة الأموال نقداً، مع تمكينهم من التصرف في حساباتهم الدائنة من أي مكان عبر شبكة الإنترنت.

وتؤدي هذه العمليات إلى ضخ كتلة نقدية مجهولة المصدر داخل الاقتصاد الوطني، وهو ما قد يترتب عنه اضطرابات اجتماعية واقتصادية خطيرة، من بينها ارتفاع الأسعار، وخلق منافسة غير متكافئة في السوق المحلي، واحتمال إضعاف العملة الوطنية، فضلاً عن توسيع الفجوة بين طبقات المجتمع.[2]

الفرع الثاني: طرق تتبع الأموال المشبوهة ودور الجهات الرقابية

إن خطورة غسل الأموال وتمويل الأنشطة غير المشروعة باستخدام العملات الرقمية لا تكمن فقط في صعوبة تحديد هوية المتعاملين، وإنما أيضاً في قدرة الجناة على نقل القيمة المالية بسرعة عبر الحدود، واستعمال محافظ رقمية ومنصات تداول قد لا تخضع دائماً للرقابة التقليدية. لذلك، لم يعد التصدي لهذه الجرائم ممكناً بالاعتماد على الوسائل الكلاسيكية وحدها، بل أصبح يتطلب منظومة رقابية تقوم على تتبع مسار الأموال، وتحليل العمليات غير الاعتيادية، وربط العناوين الرقمية بالأشخاص الطبيعيين أو المعنويين المستفيدين منها.

وقد اتجه المشرع الجزائري، من خلال القانون رقم 25-10 المعدل والمتمم للقانون رقم 05-01 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، إلى توسيع الإطار المفاهيمي والرقابي ليشمل الأصول الافتراضية، بوصفها قيماً رقمية قابلة للتداول أو التحويل أو الاستعمال في الدفع أو

1 السيد أحمد عبد الخالق، الآثار الاقتصادية والاجتماعية لتبييض الأموال، القاهرة: دار النهضة العربية، 1997، ص. 3.

2 جزول صالح، جريمة تبييض الأموال في القانون الجزائري والشريعة الإسلامية: دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة وهران، 2014-2015، ص. 80.

الاستثمار. ويُعد هذا التوسيع مهماً لأنه يسمح بإخضاع التعاملات الرقمية المشبوهة لقواعد الوقاية والرقابة، بدل تركها خارج نطاق المنظومة القانونية التقليدية.[1]

أولاً: العناية الواجبة ومعرفة هوية الزبون

تُعد العناية الواجبة أول وسيلة قانونية لتتبع الأموال المشبوهة، لأنها تسمح للمؤسسات المالية والجهات الخاضعة للرقابة بمعرفة هوية الزبون قبل الدخول معه في علاقة عمل أو تنفيذ عملية عرضية لفائدته. ولا يقتصر هذا الالتزام على الحصول على الاسم والوثائق الرسمية، بل يمتد إلى فهم طبيعة العلاقة المالية، والغرض من العملية، ومصدر الأموال، ونشاط الزبون، ومستوى المخاطر المرتبطة به.

وفي مجال العملات الرقمية، تكتسب هذه القاعدة أهمية خاصة، لأن التعامل لا يتم دائماً عبر حساب مصرفي تقليدي، بل قد يتم من خلال محافظ رقمية وعناوين مشفرة. لذلك، فإن معرفة الزبون يجب أن تشمل، إلى جانب البيانات الشخصية، كل ما يساعد على رسم ملف مخاطره، مثل مصدر الدخل، طبيعة النشاط، الغرض من التعامل، ومؤشرات استعماله للأصول الافتراضية في عمليات غير عادية.[2]

كما أن المنهج القائم على المخاطر يفرض على الجهات الخاضعة أن تميز بين الزبائن العاديين والزبائن ذوي المخاطر المرتفعة. فإذا ظهرت مؤشرات غير مألوفة، كارتفاع حجم العمليات دون مبرر اقتصادي، أو تكرار التحويلات الرقمية في مدة قصيرة، أو عدم تناسب العمليات مع نشاط الزبون، وجب تشديد إجراءات الفحص وعدم الاكتفاء بالتحقق الشكلي من الهوية.[3]

ثانياً: تحديد المستفيد الحقيقي من العمليات

لا يكفي في تتبع الأموال المشبوهة الوقوف عند الشخص الظاهر الذي يباشر العملية، لأن غسل الأموال غالباً ما يتم باستعمال واجهات قانونية أو أشخاص وسيطين لإخفاء المالك الحقيقي للأموال. لذلك، يبرز تحديد المستفيد الحقيقي كإجراء جوهري في كشف الشخص الذي يملك أو يسيطر فعلياً على الأموال أو الحساب أو المحفظة الرقمية.

---

1 قانون رقم 25-10 مؤرخ في 24 يوليو سنة 2025، يعدل ويتمم القانون رقم 05-01 المؤرخ في 6 فبراير سنة 2005 والمتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، الجريدة الرسمية للجمهورية الجزائرية، العدد 48، 24 يوليو 2025.

2 لجنة تنظيم عمليات البورصة ومراقبتها، تعليمة رقم 24-07 مؤرخة في 21 نوفمبر 2024، متضمنة تدابير اليقظة الواجبة اتجاه الزبائن في إطار الوقاية من تبييض الأموال وتمويل الإرهاب وتمويل انتشار أسلحة الدمار الشامل، ص. 3-5.

3 المرجع نفسه، ص. 2-3.

ويُقصد بالمستفيد الحقيقي الشخص الطبيعي الذي تعود إليه في النهاية السيطرة الفعلية على الزبون أو العملية، سواء كانت هذه السيطرة مباشرة أو غير مباشرة. وتظهر أهمية هذا الإجراء في حالة الشركات الوهمية أو الترتيبات القانونية المركبة، حيث قد يكون الشخص المتعامل ظاهرياً مجرد واجهة، بينما تعود المنفعة الحقيقية إلى شخص آخر يحاول إخفاء صلته بالأموال محل الشبهة.[1]

وفي سياق العملات الرقمية، يساعد تحديد المستفيد الحقيقي في الربط بين العنوان الرقمي أو المحفظة الإلكترونية وبين الشخص الذي يستعملها أو ينتفع منها. فالمحفظة الرقمية قد لا تكشف بذاتها عن هوية صاحبها، لكن تحليل المعطيات المرتبطة بها، وربطها ببيانات الزبون ومصدر الأموال وطبيعة النشاط، يسمح بتقليص دائرة الإخفاء التي يستغلها الجناة في عمليات التبييض.

ثالثاً: مراقبة العمليات غير الاعتيادية ومؤشرات الاشتباه

تقوم عملية التتبع الفعلي للأموال المشبوهة على مراقبة العمليات التي لا تنسجم مع السلوك المالي المعتاد للزبون. فالمؤسسة المالية أو الجهة الخاضعة لا تكتفي بتسجيل العملية، بل ينبغي عليها تحليلها من حيث قيمتها، وتكرارها، وأطرافها، والبلدان المرتبطة بها، والغرض الاقتصادي الظاهر منها.

وتشير المعايير الدولية إلى أن مؤشرات الاشتباه في مجال الأصول الافتراضية قد تتعلق بطبيعة العملية ذاتها، أو بنمط تكرارها، أو باستعمال أدوات تزيد من إخفاء الهوية، مثل الخلاطات الرقمية أو العملات ذات الخصوصية العالية، أو التعامل مع مناطق ضعيفة الرقابة. كما يمكن أن تنشأ الشبهة من عدم وجود مبرر اقتصادي واضح لحجم العملية أو تكرارها.[2]

وبناءً على ذلك، فإن تتبع الأموال المشبوهة في مجال العملات الرقمية يتطلب الجمع بين التحليل القانوني والتحليل التقني. فالجهات الرقابية تحتاج إلى قراءة السلوك المالي للزبون، وفي الوقت نفسه تحليل مسار التحويلات الرقمية عبر السلسلة، مثل رصد العناوين المتكررة، تتبع المحافظ المرتبطة، تحديد منصات التداول المستعملة، ومقارنة ذلك كله بالبيانات المصرح بها من طرف الزبون.

1 لمرجع نفسه، ص. 4-5.

2FATF, Virtual Assets: Red Flag Indicators of Money Laundering and Terrorist Financing, Paris: FATF/OECD, September 2020, pp. 3-5; FATF, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, Paris: FATF/OECD, October 2021, pp. 88-89.

رابعاً: الإخطار بالشبهة ودور خلية معالجة الاستعلام المالي

يمثل الإخطار بالشبهة حلقة مركزية في نظام مكافحة غسل الأموال وتمويل الأنشطة غير المشروعة. فإذا توصلت المؤسسة المالية أو الجهة الخاضعة إلى وجود مؤشرات جدية على أن العملية قد تكون مرتبطة بتبييض الأموال أو تمويل الإرهاب أو استعمال غير مشروع للأصول الرقمية، وجب عليها إخطار خلية معالجة الاستعلام المالي دون انتظار إثبات الجريمة الأصلية.

وتكمن أهمية هذا الإجراء في أنه ينقل المعلومة من مستوى المؤسسة الخاضعة إلى مستوى جهاز وطني متخصص في جمع وتحليل الاستعلامات المالية. فخلية معالجة الاستعلام المالي تقوم بدور الوسيط التحليلي بين المؤسسات المبلغة والسلطات المختصة، إذ تستقبل الإخطارات، تفحصها، تجمع المعطيات المرتبطة بها، ثم تحيل الملف عند الاقتضاء إلى الجهات القضائية أو الأمنية المختصة.

وفي مجال العملات الرقمية، يصبح الإخطار بالشبهة أكثر أهمية، لأن التحويلات قد تتم بسرعة كبيرة، وقد تنتقل الأموال من منصة إلى أخرى أو من محفظة إلى محفظة خلال وقت قصير. لذلك، فإن التأخر في الإخطار قد يؤدي إلى ضياع أثر الأموال أو تحويلها إلى أصول أخرى يصعب تعقبها.[1]

خامساً: حفظ السجلات وتبادل المعلومات بين الجهات الرقابية

لا يمكن تتبع الأموال المشبوهة دون وجود سجلات دقيقة وموثقة للعمليات والزبائن. فحفظ البيانات يسمح بالرجوع إلى تاريخ العلاقة المالية، ومعرفة تسلسل العمليات، ومقارنة التصريحات السابقة بالسلوك الفعلي للزبون. ويشمل ذلك حفظ وثائق الهوية، بيانات المستفيد الحقيقي، مصدر الأموال، طبيعة العمليات، وسائر المعلومات التي تسمح بإعادة بناء مسار الأموال عند الحاجة.

كما أن فعالية التتبع لا تتحقق داخل مؤسسة واحدة فقط، بل تتطلب تنسيقاً بين الجهات الرقابية، مثل بنك الجزائر، اللجنة المصرفية، خلية معالجة الاستعلام المالي، سلطات السوق المالي، والجهات القضائية. فجرائم غسل الأموال عبر العملات الرقمية ذات طبيعة عابرة للحدود، وقد تبدأ العملية في دولة، وتمر عبر منصة في دولة ثانية، ثم تنتهي في حساب أو أصل مادي داخل دولة ثالثة.

ومن ثم، فإن تبادل المعلومات بين السلطات الوطنية والدولية يشكل ضمانة أساسية لعدم إفلات الجناة من الرقابة. وقد أكدت المعايير الدولية أن مقدمي خدمات الأصول الافتراضية يجب أن يلتزموا

1FATF, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, pp. 88-89.

بتدابير مماثلة لتلك المفروضة على المؤسسات المالية، خاصة في ما يتعلق بمعرفة الزبون، حفظ السجلات، والإبلاغ عن العمليات المشبوهة.[1]

سادساً: الرقابة على الفئات عالية المخاطر

تزداد أهمية التتبع عندما يتعلق الأمر بالفئات التي تحمل مخاطر أعلى، مثل الأشخاص المعرضين سياسياً، أو الزبائن المرتبطين بدول ضعيفة الرقابة، أو الأشخاص الذين يستعملون هياكل قانونية معقدة لإخفاء ملكية الأموال. فهذه الحالات تتطلب عناية معززة، لأن احتمال استغلالها في تبييض الأموال أو تمويل أنشطة غير مشروعة يكون أكبر من الحالات العادية.

وقد أدخل القانون رقم 25-10 تعريفاً للأشخاص المعرضين سياسياً، بما يشمل الأشخاص الذين أوكلت إليهم وظائف عامة بارزة داخل الجزائر أو خارجها، إضافة إلى بعض المسؤولين في المنظمات الدولية. ويترتب على ذلك ضرورة إخضاع هذه الفئة لفحص أدق، خاصة من حيث مصدر الثروة، طبيعة العلاقة المالية، والغرض من العمليات المنجزة.[2]

وفي مجال العملات الرقمية، تكون الرقابة على هذه الفئات أكثر حساسية، لأن استعمال الأصول الافتراضية قد يسمح بإخفاء مصدر الأموال أو نقلها خارج القنوات المصرفية المعتادة. لذلك، فإن العناية المعززة هنا لا تهدف إلى منع التعامل بذاته، بل إلى التأكد من مشروعية مصدر الأموال وشفافية المستفيد الحقيقي من العملية.

المطلب الثالث: جرائم الاختراق وسرقة المحافظ الرقمية

أدى الانتشار المتزايد للعملات الرقمية إلى ظهور صور جديدة من الجرائم الإلكترونية، لم تعد تقتصر على الاحتيال أو غسل الأموال، بل امتدت إلى استهداف المحافظ الرقمية مباشرة، باعتبارها الوسيلة التقنية التي يحتفظ من خلالها المستخدم بمفاتيح الوصول إلى أصوله المشفرة. فالمحفظة الرقمية، سواء كانت ساخنة متصلة بالإنترنت أو باردة منفصلة عنه، لا تحتوي في حقيقتها على العملات ذاتها،

1FATF, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, pp. 80-81, 88-89.

2 قانون رقم 25-10 مؤرخ في 28 محرم عام 1447 الموافق 24 يوليو سنة 2025، يعدل ويتمم القانون رقم 05-01 المؤرخ في 27 ذي الحجة عام 1425 الموافق 6 فبراير سنة 2005، والمتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، الجريدة الرسمية للجمهورية الجزائرية، العدد 48، الصادر بتاريخ 24 يوليو 2025.

وإنما تحتوي على المفاتيح الخاصة أو العبارات السرية التي تمكّن صاحبها من التصرف في الأصول المسجلة على سلسلة الكتل.

وتكمن خطورة هذه الجرائم في أن السيطرة على المفتاح الخاص أو العبارة الاسترجاعية تعني عملياً السيطرة على الأموال الرقمية، لأن المعاملات المنفذة عبر شبكات البلوكشين تكون غالباً نهائية ويصعب إلغاؤها أو استرجاع قيمتها بعد تحويلها. لذلك، أصبح اختراق المحافظ الرقمية من أخطر صور الاعتداء على المال المعلوماتي، لأنه يجمع بين الاعتداء على نظام معلوماتي من جهة، والاستيلاء على قيمة مالية رقمية من جهة أخرى.

ولا تنفصل جرائم سرقة المحافظ الرقمية عن جرائم سرقة البيانات الإلكترونية، لأن الجاني لا يستطيع غالباً الوصول إلى المحفظة إلا عبر الاستيلاء على بيانات حساسة، مثل كلمات المرور، المفاتيح الخاصة، العبارات السرية، رموز التحقق، أو بيانات الولوج إلى منصات التداول. وقد بيّن الفقه الحديث أن سرقة البيانات الإلكترونية أصبحت تتخذ صوراً متعددة، منها الالتقاط غير المشروع للبيانات، التجسس الإلكتروني، الخداع التقني، وسرقة منفعة الحاسب الآلي.[1]

وعليه، سيتم تناول هذا المطلب من خلال فرعين؛ نخصص (الفرعالأول) لأساليب اختراق المحافظ الرقمية، بينما نخصص(الفرع الثاني) لوسائل الحماية وإثبات جريمة الاختراق.

الفرع الأول: أساليب اختراق المحافظ الرقمية

تتعدد أساليب اختراق المحافظ الرقمية بحسب نوع المحفظة، ومستوى حماية المستخدم، وطبيعة النظام أو المنصة المستعملة. وقد يكون الاختراق موجهاً إلى جهاز الضحية مباشرة، أو إلى بياناته السرية، أو إلى منصة التداول التي يحتفظ من خلالها بأصوله الرقمية. ويجمع هذه الأساليب هدف واحد، يتمثل في تمكين الجاني من الحصول على مفاتيح الوصول أو نقل الأصول إلى محافظ يسيطر عليها.

أولاً: الالتقاط غير المشروع للبيانات الرقمية

يُعد الالتقاط غير المشروع للبيانات الرقمية من أخطر الوسائل المستعملة في سرقة المحافظ الرقمية. ويقصد به اطلاع الجاني أو حصوله على بيانات يتم إرسالها عبر الشبكة المعلوماتية أو من

1 بودقزدام سامية، ونويس نبيل، "سرقة البيانات الإلكترونية: دراسة تأصيلية مقارنة بين الأحكام الشرعية والقانون الجزائري"، مجلة الدراسات القانونية والاقتصادية، المجلد 08، العدد 02، 2025، ص. 191-194.

خلال جهاز إلكتروني، دون إذن قانوني أو مبرر مشروع. وتزداد خطورة هذا الأسلوب عندما تكون البيانات الملتقطة مرتبطة بمحفظة رقمية، ككلمة المرور، المفتاح الخاص، العبارة السرية، أو رمز المصادقة الثنائية.

وقد يتحقق هذا الالتقاط من خلال اعتراض الاتصال بين المستخدم والمنصة، أو من خلال برامج خبيثة مزروعة داخل الجهاز، أو عبر شبكات غير آمنة تسمح بتتبع البيانات المرسلة. وفي جميع الأحوال، فإن خطورة الالتقاط تكمن في أنه يتم غالباً دون علم الضحية، مما يسمح للجاني باستعمال البيانات لاحقاً في الدخول إلى المحفظة أو تحويل الأصول الرقمية.

وتجد هذه الصورة سندها في التحليل القانوني لجرائم سرقة البيانات الإلكترونية، حيث يُنظر إلى الحصول غير المشروع على البيانات المرسلة عبر الشبكات باعتباره اعتداءً مباشراً على السرية المعلوماتية، خاصة إذا تعلق الأمر ببيانات مالية أو بيانات ولوج ذات قيمة اقتصادية.[1]

ثانياً: التجسس الإلكتروني وبرامج سرقة المفاتيح

يتحقق التجسس الإلكتروني باستعمال برامج أو أدوات تقنية تسمح للجاني بالاطلاع الخفي على معلومات الضحية ونشاطه الرقمي. وفي مجال المحافظ الرقمية، قد تأخذ هذه البرامج شكل برمجيات خبيثة قادرة على تسجيل ضغطات لوحة المفاتيح، أو التقاط صور للشاشة، أو البحث داخل الجهاز عن ملفات تحتوي على مفاتيح خاصة أو عبارات استرجاع.

وتكمن خطورة هذا الأسلوب في أن الضحية قد يستمر في استعمال جهازه بصورة عادية دون أن يعلم بوجود برنامج يتجسس عليه. فإذا كتب عبارة الاسترجاع، أو حفظ صورة لها، أو قام بنسخ عنوان محفظة، أصبح الجاني قادراً على الوصول إلى هذه البيانات واستعمالها في سرقة الأصول الرقمية.

وقد أشار الفقه إلى أن التجسس المعلوماتي يقوم على كشف واستظهار حقائق مخفية بطريقة غير مشروعة، من خلال برامج تتيح لقراصنة الإنترنت الاطلاع على بيانات الأشخاص أو المؤسسات واستغلالها في أنشطة إجرامية.[2] وتزداد خطورة هذا الفعل إذا كانت البيانات المستهدفة مالية أو تجارية أو أمنية، وهو ما ينطبق على بيانات المحافظ الرقمية التي تمثل مفتاح التصرف في أموال مشفرة.

---

[1] بودقزدام سامية، ونويس نبيل ، مرجع سبق ذكره ، ص191.

[2] المرجع نفسه، ص. 191-192.

ثالثاً: الخداع التقني والتصيد الاحتيالي

يُعد التصيد الاحتيالي من أكثر الأساليب شيوعاً في سرقة المحافظ الرقمية. ويقوم هذا الأسلوب على إنشاء مواقع أو صفحات أو رسائل وهمية تشبه المواقع الأصلية لمنصات التداول أو تطبيقات المحافظ، بهدف دفع المستخدم إلى إدخال بياناته السرية، مثل كلمة المرور أو العبارة الاسترجاعية. وبمجرد إدخال هذه البيانات، تنتقل إلى الجاني الذي يستعملها لاحقاً للوصول إلى المحفظة أو تحويل الأصول.

ويمثل هذا الأسلوب امتداداً لما عُرف في جرائم سرقة البيانات باسم **أسلوب الخداع**، حيث يقوم قراصنة الإنترنت بإنشاء مواقع وهمية مشابهة للمواقع الأصلية للشركات والمؤسسات التجارية، فتظهر للضحية كأنها مواقع حقيقية، مما يؤدي إلى استقبال الجناة للمعاملات والبيانات المالية والتجارية، ومن بينها بيانات بطاقات الدفع أو وسائل الولوج الإلكترونية.[1]

وفي مجال العملات الرقمية، يصبح الخداع أكثر خطورة لأن بعض المستخدمين قد يجهلون أن المنصات الشرعية لا تطلب أبداً الإفصاح عن العبارة السرية للمحفظة. فإذا وقع المستخدم في فخ موقع مزيف أو رابط احتيالي، فقد يمنح الجاني السيطرة الكاملة على محفظته دون حاجة إلى كسر تقني مباشر.

رابعاً: اختراق قواعد البيانات ومنصات التداول

لا يستهدف الجناة المستخدم الفرد فقط، بل قد يهاجمون قواعد البيانات الكبرى الخاصة بمنصات التداول أو شركات الخدمات الرقمية. ويقصد بخرق البيانات وقوع حادث أمني يؤدي إلى تسريب معلومات المستخدمين، مثل الأسماء، عناوين البريد الإلكتروني، أسماء المستخدمين، كلمات المرور، أو المعلومات المالية، وهي بيانات يمكن توظيفها لاحقاً للوصول إلى المحافظ أو تنفيذ عمليات احتيالية.

وتحدث خروقات البيانات نتيجة عوامل متعددة، منها البرمجيات الخبيثة، التصيد الاحتيالي، كلمات المرور الضعيفة، الثغرات التقنية في البرمجيات، أو حتى تواطؤ بعض الموظفين من الداخل. وقد تؤدي

[1] بودقزدام سامية، ونويس نبيل ، مرجع سبق ذكره ،ص. 193-194.

هذه الخروقات إلى بيع البيانات في الشبكة المظلمة، أو استعمالها في هجمات لاحقة أكثر دقة تستهدف المحافظ الرقمية للأشخاص الذين ثبت امتلاكهم أصولاً مشفرة.[1]

وتؤكد التقارير الحديثة المتعلقة بجرائم العملات الرقمية أن سرقة الأصول المشفرة عبر الاختراقات لا تزال تشكل خطراً مرتفعاً، إذ أشار تقرير نُقل عن (Chainalysis)إلى أن قيمة العملات الرقمية المسروقة عبر الاختراقات سنة 2024 بلغت حوالي 2.2 مليار دولار، مع تسجيل 303 حادثة اختراق، وأن كثيراً من هذه السرقات ارتبط باختراق المفاتيح الخاصة واستهداف منصات مركزية .

خامساً: سرقة منفعة الحاسب الآلي واستغلال الجهاز في الجريمة

لا تنحصر سرقة المحافظ الرقمية في الاستيلاء المباشر على المفتاح الخاص، بل قد تتم أيضاً من خلال استغلال جهاز الضحية أو قدراته التقنية دون إذن. وتظهر هنا فكرة **سرقة منفعة الحاسب الآلي**، التي تعني الانتفاع غير المشروع بخدمة إلكترونية أو بقدرة نظام معلوماتي دون نية تملك الجهاز ذاته.

وفي مجال العملات الرقمية، قد يستغل الجاني جهاز الضحية لتسهيل الدخول إلى حسابات محفوظة، أو تمرير عمليات مشبوهة، أو تعدين عملات رقمية دون علمه، أو استعمال الجهاز كوسيط لإخفاء أثر الجريمة. وهذا النمط يختلف عن السرقة التقليدية، لأنه لا ينصب على شيء مادي ملموس، بل على منفعة رقمية لها قيمة اقتصادية، مما يفرض توسيع النظر القانوني إلى مفهوم المال والمنفعة في البيئة الرقمية.[2]

الفرع الثاني: وسائل الحماية وإثبات جريمة الاختراق

إن خطورة جرائم اختراق المحافظ الرقمية لا تقتصر على سهولة تنفيذ بعض صورها، بل تمتد إلى صعوبة إثباتها، لأن الجريمة تقع في فضاء رقمي عابر للحدود، وقد تُنفذ بواسطة هويات مستعارة، أو عناوين محافظ لا تكشف بذاتها عن صاحبها الحقيقي. لذلك، لا بد من الجمع بين الحماية التقنية الوقائية من جهة، والإثبات الجنائي الرقمي من جهة أخرى.

أولاً: وسائل الحماية التقنية للمحافظ الرقمية

[1] لمرجع نفسه، ص. 191.

[2] المرجع نفسه، ص. 194.

تبدأ الحماية الفعالة للمحفظة الرقمية من إدراك أن المفتاح الخاص أو العبارة الاسترجاعية يمثلان جوهر السيطرة على الأصول الرقمية. ولذلك، فإن أول واجب وقائي يتمثل في عدم حفظ هذه البيانات في صور رقمية يسهل اختراقها، وعدم إرسالها عبر البريد الإلكتروني أو تطبيقات المراسلة أو المواقع الإلكترونية، وعدم إدخالها في أي صفحة إلا داخل تطبيق موثوق ومتحقق منه.

كما يُعد استعمال المصادقة الثنائية من الوسائل الضرورية لحماية حسابات التداول، بشرط ألا تكون الرسائل النصية وحدها هي الوسيلة المعتمدة، لأن بعض الجرائم قد تتم عبر الاستيلاء على رقم الهاتف أو إعادة إصدار الشريحة. ويُفضل في هذا السياق استعمال تطبيقات تحقق مستقلة أو مفاتيح حماية مادية، إلى جانب كلمات مرور قوية وفريدة لكل منصة[1].

وتدخل ضمن وسائل الحماية كذلك ضرورة تحديث الأنظمة والتطبيقات بصفة مستمرة، وتجنب تحميل محافظ أو إضافات متصفح من مصادر غير رسمية، وعدم استعمال شبكات عامة غير آمنة عند الدخول إلى الحسابات المالية. كما ينبغي فصل الأصول طويلة الأجل في محافظ باردة غير متصلة بالإنترنت، مع الاحتفاظ بنسخ آمنة من العبارة السرية في أماكن محمية.

وتنسجم هذه الإجراءات مع ما تقرره الدراسات الخاصة بسرقة البيانات الإلكترونية، التي تؤكد أهمية استعمال كلمات مرور قوية ومختلفة، تحديث الأنظمة باستمرار، تفادي محطات USB العامة، مراقبة الحسابات، وتجنب تخزين البيانات غير الضرورية.

ثانياً: الحماية القانونية للبيانات الشخصية والأمن الرقمي

لا تكفي الحماية التقنية وحدها، لأن اختراق المحافظ الرقمية يمثل في كثير من الحالات اعتداءً على بيانات شخصية ومالية. وفي هذا السياق، يُعد القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي إطاراً قانونياً مهماً لحماية البيانات المرتبطة بالمستخدمين، خاصة من حيث فرض مبادئ المشروعية، الموافقة، السرية، وأمن المعالجة.

ويفرض هذا القانون على المسؤول عن المعالجة اتخاذ الاحتياطات اللازمة لحماية المعطيات من الإتلاف أو الفقدان أو الكشف أو الولوج غير المرخص. وتظهر أهمية هذا الالتزام بالنسبة للمنصات أو الجهات التي تحتفظ ببيانات المستخدمين أو وثائقهم أو معلومات الولوج إلى خدمات مالية رقمية، لأن أي

[1] جيدول محمد، وعباس حمزة، "حماية الخصوصية والأمن الرقمي في القانون الجنائي"، مجلة الميدان للعلوم الإنسانية والاجتماعية، المجلد 07، العدد 2026، 2026، ص 30-31.

إهمال في حماية هذه البيانات قد يسهل جرائم الاختراق وسرقة المحافظ. وقد ورد القانون رقم 18-07 في الجريدة الرسمية الجزائرية، العدد 34 لسنة 2018، وهو ينظم حماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي.

أما من الناحية الجنائية، فإن الاعتداء على المحافظ الرقمية قد يدخل ضمن جرائم المساس بأنظمة المعالجة الآلية للمعطيات، خاصة إذا تحقق الولوج أو البقاء غير المشروع داخل نظام معلوماتي، أو تم حذف أو تعديل أو نسخ بيانات، أو استعملت وسائل احتيالية للحصول على منفعة مالية. وتزداد جسامة الفعل إذا ترتب عنه تحويل أصول رقمية أو تعطيل حسابات أو إتلاف بيانات مرتبطة بالضحية[1].

ثالثاً: الإطار الجزائري لمكافحة جرائم تكنولوجيا الإعلام والاتصال

إلى جانب قانون العقوبات، جاء القانون رقم 09-04 ليضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. ويظهر من نص هذا القانون أنه يهدف إلى وضع قواعد خاصة للوقاية من الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال، كما يعرّف الجرائم المرتبطة بهذه التكنولوجيا بأنها الجرائم التي تمس أنظمة المعالجة الآلية للمعطيات وغيرها من الجرائم التي تُرتكب أو يُسهل ارتكابها بواسطة منظومة معلوماتية أو نظام اتصال إلكتروني[2] .

وتظهر أهمية هذا القانون في مجال المحافظ الرقمية من زاويتين: الأولى وقائية، لأنه يتيح وضع آليات خاصة لمكافحة الجرائم المعلوماتية؛ والثانية إجرائية، لأنه يقر قواعد تتعلق بالمراقبة، التفتيش، الحجز، والتعاون الدولي. كما ينص القانون على إنشاء جهاز وطني للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، يتولى تنسيق عمليات الوقاية والمساعدة في التحقيقات وتبادل المعلومات مع الجهات الأجنبية قصد تحديد مرتكبي الجرائم المعلوماتية .

وبذلك، فإن جرائم اختراق المحافظ الرقمية لا ينبغي النظر إليها كواقعة تقنية معزولة، بل كجريمة معلوماتية قد تتطلب تدخلاً مؤسسياً متخصصاً يجمع بين الخبرة التقنية والتحقيق الجنائي والتعاون الدولي[3].

---

[1] القانون رقم 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، العدد 34، الصادر بتاريخ 10 يونيو 2018،

[2] القانون رقم 09-04 المؤرخ في 5 أغسطس 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، 16 أغسطس 2009.

[3] جيدول محمد، وعباس حمزة، مرجع سبق ذكره، ص30.

رابعاً: إثبات جريمة الاختراق بالأدلة الرقمية

يقوم إثبات جريمة اختراق المحفظة الرقمية على جمع الأدلة الرقمية بطريقة تحفظ سلامتها وقيمتها القانونية. ومن أهم هذه الأدلة سجلات الدخول إلى الحسابات، عناوين الإنترنت المستعملة، بيانات الأجهزة، سجلات المنصة، رسائل التصيد، الملفات الخبيثة، عناوين المحافظ التي استقبلت الأموال، ومسار التحويلات على سلسلة الكتل.

وتتميز جرائم العملات الرقمية بأن جزءاً من أثرها يبقى ظاهراً على البلوكشين، لأن التحويلات تُسجل في دفتر عام يمكن تتبع مساره. غير أن هذا لا يعني سهولة تحديد الجاني، لأن العنوان الرقمي لا يكشف بالضرورة عن هوية الشخص. لذلك، يجب الجمع بين تحليل السلسلة من جهة، والحصول على بيانات المنصات ومزودي الخدمات من جهة أخرى، حتى يمكن الربط بين العنوان الرقمي والفاعل الحقيقي.

وقد أكدت المعايير الدولية، ومنها اتفاقية بودابست، أهمية أدوات التحقيق الرقمي مثل الحفظ السريع للبيانات المخزنة، أوامر تقديم البيانات، تفتيش وحجز البيانات المخزنة، وجمع بيانات المرور في الوقت الحقيقي. وتنص الاتفاقية على تمكين السلطات من حفظ البيانات الإلكترونية المعرضة للفقد أو التعديل، والبحث في الأنظمة المعلوماتية وحجز أو نسخ البيانات مع الحفاظ على سلامتها[1] .

خامساً: مؤشرات الاشتباه وتتبع الأموال المسروقة

بعد وقوع الاختراق، لا يقتصر دور التحقيق على إثبات الدخول غير المشروع، بل يمتد إلى تتبع الأموال الرقمية المسروقة. وتفيد مؤشرات الاشتباه الصادرة عن مجموعة العمل المالي FATF في رصد بعض الأنماط التي قد تدل على استعمال الأصول الافتراضية في نشاط إجرامي، مثل تعدد التحويلات بسرعة، استعمال خدمات تزيد من إخفاء الهوية، نقل الأموال بين عدة محافظ، أو تحويلها إلى منصات في دول ضعيفة الرقابة. وقد أوضحت FATF أن مؤشرات الأصول الافتراضية تستند إلى أكثر من مئة دراسة حالة وتجارب عملية في تتبع إساءة استخدام الأصول الافتراضية[2] .

وتظهر أهمية هذه المؤشرات في جرائم سرقة المحافظ الرقمية، لأن الجاني غالباً لا يحتفظ بالأموال في المحفظة الأولى التي استقبلتها، بل ينقلها عبر سلسلة من العناوين والمنصات أو يحاول

[1] جيدول محمد، وعباس حمزة ، مرجع نفسه ، ص31.

[2]FATF, Virtual Assets: Red Flag Indicators of Money Laundering and Terrorist Financing, Paris: FATF/OECD, September 2020, pp. 5-12.

تحويلها إلى عملات أخرى لتضليل التتبع. لذلك، فإن سرعة التبليغ والتجميد والتعاون مع منصات التداول تمثل عناصر أساسية لزيادة إمكانية استرجاع الأموال أو تحديد الجاني.

سادساً: عبء الإثبات ومسؤولية الضحية والمنصة

تثير جرائم اختراق المحافظ الرقمية إشكالاً دقيقاً يتعلق بتحديد المسؤولية: هل كان الاختراق بسبب إهمال الضحية في حفظ مفاتيحه؟ أم بسبب ضعف حماية المنصة؟ أم بسبب فعل خارجي إجرامي مستقل؟ لذلك، يجب على التحقيق أن يميز بين الحالات المختلفة، لأن لكل حالة آثاراً قانونية مختلفة.

فإذا ثبت أن الجاني حصل على بيانات الضحية عبر تصيد احتيالي أو برنامج خبيث، فإن المسؤولية الجنائية تقوم في حقه متى ثبتت العلاقة السببية بين الفعل والنتيجة. أما إذا كان الاختراق نتيجة خرق في قاعدة بيانات منصة تداول، فقد تثور إلى جانب المسؤولية الجنائية مسؤولية مدنية أو تنظيمية عن ضعف التدابير الأمنية، خاصة إذا كانت المنصة تحتفظ ببيانات شخصية أو مالية ولم تتخذ الاحتياطات اللازمة لحمايتها.

ومن الناحية العملية، يحتاج إثبات هذه الجرائم إلى خبرة رقمية متخصصة، تحفظ الدليل من العبث، وتحدد زمن الاختراق، وطريقة الدخول، ومسار الأموال، والأجهزة أو العناوين المرتبطة بالجريمة. ولا يكون الدليل الرقمي مقنعاً إلا إذا تم جمعه وفق إجراءات تحافظ على سلامته وسلسلة حيازته، حتى لا يثار الدفع بتغييره أو اصطناعه[1].

المبحث الثاني:الأليات القانونية لمواجهة جرائم العملات الرقمية

لا تكتمل الدراسة القانونية لجرائم العملات الرقمية بمجرد تحديد صورها وأساليب ارتكابها، بل لا بد من الانتقال إلى بحث آليات المواجهة التي يمكن من خلالها الحد من خطورتها وملاحقة مرتكبيها. فإذا كان المبحث السابق قد كشف عن تنوع الأنماط الإجرامية المرتبطة بالأصول المشفرة، فإن هذا المبحث يهدف إلى دراسة الوسائل القانونية والقضائية والتقنية التي يمكن اعتمادها لمواجهة هذه الجرائم، سواء من خلال التجريم والتنظيم، أو من خلال المتابعة القضائية والتحقيق، أو من خلال تطوير أدوات الحجز والإثبات الرقمي.

[1] –جديول محمد ، و عباس حمزة، مرجع سابق ص 32.

وتبرز أهمية هذا المبحث في أن جرائم العملات الرقمية لا يمكن التعامل معها بالوسائل التقليدية وحدها، نظراً لطبيعتها التقنية المعقدة، واعتمادها على مفاهيم مستحدثة مثل المحافظ الرقمية، المفاتيح الخاصة، العناوين المشفرة، والمنصات اللامركزية. كما أن هذه الجرائم غالباً ما تتجاوز الحدود الوطنية، الأمر الذي يفرض ضرورة تفعيل آليات التعاون، وتطوير قدرات الجهات القضائية والأمنية، وتحيين النصوص القانونية بما يواكب تطور التكنولوجيا المالية.

وعليه، سيتم تناول هذا المبحث من خلال ثلاثة مطالب مترابطة. يُخصص **(المطلب الأول)** لدراسة المواجهة التشريعية، من خلال تحليل النصوص القانونية التي اتجهت إلى ضبط استعمال العملات الرقمية وتجريم السلوكيات المرتبطة بها. أما **(المطلب الثاني)** فيتناول المواجهة القضائية، مع التركيز على دور القضاء والأقطاب الجزائية المتخصصة في متابعة الجرائم الرقمية، خاصة في ظل ما أظهرته الدراسات من عجز الآليات القضائية التقليدية عن استيعاب تعقيدات الإجرام المعلوماتي الحديث. في حين يُخصص **(المطلب الثالث)** لدراسة التحديات التقنية وسبل تطوير آليات المواجهة، ولا سيما ما يتعلق بحجز ومصادرة العملات الافتراضية، وتتبع العائدات الإجرامية، واستخراج الأدلة الإلكترونية الحساسة، مثل المفاتيح الخاصة والبيانات الرقمية المرتبطة بالمعاملات.

المطلب الأول: المواجهة التشريعية لجرائم العملات الرقمية

أفرزت العملات الرقمية واقعاً قانونياً جديداً لم تعد معه النصوص الجنائية التقليدية كافية وحدها لمواجهة المخاطر المستحدثة، بالنظر إلى الطبيعة اللامادية لهذه العملات، وسهولة تداولها عبر الحدود، وإمكانية توظيفها في غسل الأموال، وتمويل الأنشطة غير المشروعة، والاحتيال الإلكتروني، والتهرب من الرقابة المصرفية. لذلك اتجهت السياسة التشريعية، خاصة في الجزائر، إلى اعتماد مقاربة مزدوجة: تقوم من جهة على **تجريم السلوكيات المرتبطة بالعملات الرقمية** ، ومن جهة أخرى على **تنظيم أو حظر استخدامها وتداولها** متى شكلت تهديداً للنظام المالي والأمن الاقتصادي. وقد ظهر هذا التوجه بدايةً من قانون المالية لسنة 2018، الذي نص صراحة على منع شراء العملة الافتراضية وبيعها واستعمالها وحيازتها، ثم تعزز لاحقاً بموجب القانون رقم 25-10 المعدل والمتمم لقانون الوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما.[1]

1 قانون رقم 17-11 مؤرخ في 27 ديسمبر 2017، يتضمن قانون المالية لسنة 2018، الجريدة الرسمية للجمهورية الجزائرية، العدد 76، الصادر بتاريخ 28 ديسمبر 2017، وكذا القانون رقم 25-10 مؤرخ في 24 يوليو 2025، يعدل ويتمم القانون رقم 05-01

وعليه، سيتم تناول هذا المطلب من خلال فرعين: نخصص(**الفرع الأول**)لدراسة تجريم السلوكيات المرتبطة بالعملات الرقمية، ثم نتناول في(**الفرع الثاني**)تنظيم استخدام وتداول العملات الرقمية في التشريع الجزائري.

الفرع الأول: تجريم السلوكيات المرتبطة بالعملات الرقمية

تقوم المواجهة التشريعية لجرائم العملات الرقمية على فكرة أساسية مفادها أن الخطر لا يكمن في التقنية في ذاتها، بل في الأفعال غير المشروعة التي يمكن أن تُرتكب بواسطتها أو من خلالها. فالعملة الرقمية، بسبب اعتمادها على التشفير وإمكانية تداولها خارج القنوات البنكية التقليدية، قد تتحول إلى وسيلة لإخفاء مصدر الأموال، أو نقل القيمة المالية بعيداً عن الرقابة، أو تمويل أنشطة إجرامية يصعب تتبعها بالوسائل الكلاسيكية. لذلك لم يعد التجريم مقتصراً على صور غسل الأموال وتمويل الإرهاب التقليدية، بل امتد ليشمل صوراً جديدة مرتبطة بإصدار العملات الافتراضية، وتداولها، وتحويلها، واستخدامها كوسيلة دفع أو استثمار غير مرخص.[1]

وقد تبنى المشرع الجزائري منذ سنة 2018 موقفاً صارماً من العملات الافتراضية، حيث نصت المادة 117 من قانون المالية لسنة 2018 على أنه: «يمنع شراء العملة الافتراضية وبيعها واستعمالها وحيازتها»، كما عرّفت العملة الافتراضية بأنها تلك التي يستعملها مستخدمو الإنترنت عبر الشبكة، وتتميز بغياب الدعامة المادية كالقطع والأوراق النقدية ووسائل الدفع التقليدية. ويُفهم من هذا النص أن المشرع لم يكتفِ بمنع التداول التجاري، بل وسّع نطاق الحظر ليشمل مجرد الحيازة والاستعمال، وهو توجه يعكس الطابع الوقائي الصارم للسياسة التشريعية الجزائرية في هذا المجال.[2]

غير أن الإشكال الذي طُرح بخصوص نص المادة 117 يتمثل في أن الحظر الوارد فيها لم يكن مصحوباً ببناء جنائي تفصيلي يحدد بدقة أركان الجريمة، وصور السلوك المجرم، والعقوبات المناسبة، إذ اكتفى النص بالإحالة إلى القوانين والتنظيمات المعمول بها. وهذا ما جعل جزءاً من الفقه يعتبر أن

المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، الجريدة الرسمية للجمهورية الجزائرية، العدد 48، الصادر بتاريخ 24 يوليو 2025.

1 هواري قعموسي، "تجريم العملة الافتراضية الرقمية بقانون تبييض الأموال رقم 25-10 بالجزائر"، المجلة الجزائرية للحقوق والعلوم السياسية، 2025، ص. 515-516.

2 قانون رقم 17-11، يتضمن قانون المالية لسنة 2018، المادة 117، الجريدة الرسمية، العدد 76.

التجريم في هذه المرحلة كان أقرب إلى الحظر العام منه إلى التجريم الجنائي المكتمل، خصوصاً في ظل غياب نص خاص يربط العملات الرقمية صراحة بجرائم غسل الأموال وتمويل الإرهاب.[1]

وقد حاول المشرع تجاوز هذا النقص من خلال القانون رقم 25-10، المعدل والمتمم للقانون رقم 05-01 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما. وتكمن أهمية هذا التعديل في أنه نقل التعامل مع العملات الرقمية من مجرد حظر مالي أو نقدي إلى مجال أكثر خطورة، وهو مجال مكافحة الجرائم المالية المنظمة، بما يعني إدماج الأصول الافتراضية ضمن السياسة الجنائية لمكافحة غسل الأموال وتمويل الإرهاب. ويؤكد ذلك ما ذهبت إليه الدراسات الحديثة التي اعتبرت أن القانون رقم 25-10 يمثل مرحلة جديدة في تجريم العملة الافتراضية الرقمية في الجزائر، لكونه يربطها مباشرة بمخاطر تمويل الإرهاب وتبييض الأموال.[2]

وعليه، يمكن القول إن السلوكيات المجرمة في هذا المجال لا تنحصر في فعل واحد، بل تشمل مجموعة من الأفعال المتداخلة، مثل: إصدار العملات الرقمية أو الترويج لها دون ترخيص، بيعها أو شراؤها، استعمالها كوسيلة للدفع، تحويلها بقصد إخفاء مصدر الأموال، الوساطة في تداولها، أو إنشاء منصات غير مرخصة لتبادلها. كما يمكن أن تأخذ الجريمة صورة الاشتراك أو المساعدة، كأن يقوم شخص بتوفير محافظ رقمية، أو عناوين مشفرة، أو حسابات وسيطة لتسهيل نقل الأموال ذات المصدر غير المشروع. وهنا تظهر خصوصية الركن المادي في جرائم العملات الرقمية، لأنه قد يتحقق عبر عمليات تقنية لا تترك أثراً مادياً مباشراً، وإنما تترك أثراً رقمياً يحتاج إلى خبرة فنية لإثباته.[3]

أما من حيث الركن المعنوي، فإن أغلب هذه الجرائم تفترض توافر القصد الجنائي، أي علم الجاني بالطبيعة غير المشروعة للنشاط الذي يقوم به، واتجاه إرادته إلى استعمال العملة الرقمية خارج الإطار القانوني أو بقصد إخفاء الأموال وتمويه مصدرها. غير أن إثبات هذا القصد قد يكون صعباً في بعض الحالات، خاصة إذا دفع المتهم بأنه كان يجهل الحظر القانوني أو يعتقد أنه يقوم باستثمار رقمي عادي. ولهذا تبدو أهمية القرائن الرقمية، مثل تكرار العمليات، استخدام منصات مجهولة، التعامل بمحافظ غير

1 فريدة حداد وعبد الحق قريمس، "العملة الافتراضية في القانون الجزائري"، المجلة الجزائرية للعلوم القانونية والسياسية، ص.385.

2 قعموسي ، مرجع سبق ذكره ، ص519-520.

3مرجع نفسه ص521.

موثقة، أو تقسيم التحويلات إلى مبالغ صغيرة، باعتبارها مؤشرات قد تساعد جهات التحقيق في إثبات الطابع الإجرامي للسلوك.

ومن ثم، فإن التجريم التشريعي للعملات الرقمية في الجزائر يقوم على منطق وقائي واضح: فالمشرع لا ينتظر وقوع غسل الأموال أو تمويل الإرهاب فعلياً، بل يتدخل منذ مرحلة التداول أو الحيازة أو الاستعمال غير المرخص، بهدف سد المنافذ التي قد يستغلها الجناة لإدماج الأموال غير المشروعة في الدورة الاقتصادية.

الفرع الثاني: تنظيم استخدام وتداول العملات الرقمية

إذا كان التجريم يمثل الجانب الردعي في مواجهة جرائم العملات الرقمية، فإن التنظيم يمثل الجانب الوقائي والرقابي. غير أن المشرع الجزائري لم يتجه، في المرحلة الحالية، إلى تنظيم تداول العملات الرقمية وفق نظام الترخيص كما فعلت بعض التشريعات المقارنة، بل اختار سياسة الحظر. ويظهر ذلك بوضوح في المادة 117 من قانون المالية لسنة 2018، التي منعت شراء العملة الافتراضية وبيعها واستعمالها وحيازتها، مما يعني أن الأصل في التعامل بهذه العملات داخل الجزائر هو المنع لا الإباحة.[1]

ويرجع هذا الاتجاه إلى عدة اعتبارات قانونية واقتصادية. فمن الناحية القانونية، تفتقر العملات الرقمية اللامركزية إلى جهة إصدار رسمية، ولا تخضع لإشراف بنك مركزي، كما أن قيمتها تتحدد غالباً وفق العرض والطلب في الأسواق الرقمية، وهو ما يجعلها بعيدة عن الضمانات المرتبطة بالنقود القانونية. ومن الناحية الاقتصادية، يشكل تداولها خطراً على السياسة النقدية، لكونها تسمح بتحويل القيمة المالية خارج النظام المصرفي، وقد تُستعمل للتهرب من قواعد الصرف، أو إخراج رؤوس الأموال بطرق غير خاضعة للرقابة.[2]

ومع ذلك، يجب التمييز بين **العملات الافتراضية الخاصة** ، مثل العملات المشفرة المتداولة عبر منصات رقمية، وبين **العملة الرقمية الرسمية** التي قد يصدرها البنك المركزي. فالقانون النقدي والمصرفي رقم 23-09 فتح المجال أمام فكرة الدينار الرقمي أو العملة الرقمية للبنك المركزي، وهو توجه يختلف جذرياً عن العملات الافتراضية اللامركزية، لأن العملة الرقمية الرسمية تبقى صادرة عن سلطة نقدية

1المادة 117 من قانون رقم 17-11، المتضمن قانون المالية لسنة 2018.

2 حداد وقريمس ، مرجع سابق ، ص383

وطنية وتخضع لرقابتها. ولذلك لا يجوز الخلط بين الحظر المفروض على العملات الافتراضية غير الرسمية وبين إمكانية تطوير أدوات دفع رقمية رسمية داخل النظام المصرفي الوطني. [1]

وتبرز أهمية التنظيم كذلك في إلزام المؤسسات المالية والمصرفية باتخاذ تدابير يقظة خاصة تجاه العمليات المرتبطة بالأصول الافتراضية. وقد اتجه بنك الجزائر، وفق ما ورد في الخطوط التوجيهية الحديثة، إلى تحديد إجراءات التعرف على العمليات المرتبطة بالأصول الافتراضية ووقفها وحظرها، وذلك ضماناً للتطبيق الصارم لمقتضيات الحظر المنصوص عليه في القوانين الوطنية، خاصة في مجال مكافحة تبييض الأموال وتمويل الإرهاب.

ويتوافق هذا التوجه مع المعايير الدولية الصادرة عن مجموعة العمل الماليFATF ، التي تعتبر أن الأصول الافتراضية ومقدمي خدماتها يطرحون مخاطر جدية في مجال غسل الأموال وتمويل الإرهاب، وتوصي الدول بإخضاع مقدمي خدمات الأصول الافتراضية للتسجيل أو الترخيص والرقابة، مع تطبيق تدابير العناية الواجبة وتتبع التحويلات. غير أن الجزائر، بدلاً من تبني نموذج الترخيص، اختارت في المرحلة الحالية نموذج الحظر والرقابة الوقائية، وهو خيار يمكن تبريره بضعف الإطار التقني والرقابي اللازم لمتابعة هذا النوع من المعاملات.[2]

وعليه، فإن تنظيم استخدام وتداول العملات الرقمية في الجزائر لا يقوم على الاعتراف بها كأداة قانونية للتبادل، بل على منعها ومراقبة أي نشاط يرتبط بها. ويترتب على ذلك أن أي تداول أو استعمال أو حيازة للعملات الافتراضية قد يشكل مخالفة قانونية، وقد يأخذ وصفاً جنائياً أشد إذا ارتبط بغسل الأموال، أو تمويل الإرهاب، أو الاحتيال، أو تهريب رؤوس الأموال. ومن هنا، يظهر أن المشرع الجزائري اعتمد مقاربة احترازية صارمة، تقوم على حماية النظام المالي الوطني قبل التفكير في دمج العملات الرقمية ضمن الاقتصاد الرسمي.

1جلول شرارة، وليلى أسمهان بقبق، "العملات الرقمية للبنوك المركزية: تحديات ومتطلبات الدينار الرقمي الجزائري في ظل القانون النقدي والمصرفي 23-09"، مجلة طبنة للدراسات العلمية الأكاديمية، المركز الجامعي سي الحواس بريكة، مج. 6، ع. 2، 2023، ص 111.

2Financial Action Task Force (FATF), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, Paris: FATF/OECD, 2021, pp. 15-16.

المطلب الثاني: المواجهة القضائية

لا تكفي المواجهة التشريعية وحدها للحد من جرائم العملات الرقمية، ما لم تُدعّم بمواجهة قضائية فعالة قادرة على تحريك الدعوى العمومية، مباشرة التحقيق، جمع الأدلة الرقمية، وتكييف الأفعال المرتكبة تكييفاً قانونياً دقيقاً. فالجرائم المرتبطة بالعملات الرقمية لا تظهر غالباً في صورة مادية تقليدية، بل تتحقق عبر فضاء رقمي عابر للحدود، من خلال محافظ إلكترونية، عناوين مشفرة، منصات تداول، وتحويلات يصعب تتبعها بالوسائل الكلاسيكية.

وتكمن خصوصية المواجهة القضائية لهذه الجرائم في أنها تتطلب قضاءً متخصصاً، وضبطية قضائية مؤهلة، وآليات تحقيق رقمية تحفظ الدليل من الضياع أو التلاعب. لذلك تدخل المشرع الجزائري لتوسيع الاختصاص القضائي في الجرائم المعقدة، ثم استحدث قطباً جزائياً وطنياً مختصاً بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بما يسمح بمواجهة الجرائم الرقمية ذات الطابع المتشعب والعابر للاختصاصات المحلية التقليدية. وقد ورد القانون رقم 09-04 بوصفه إطاراً خاصاً للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، [1] بينما حدد المرسوم التنفيذي رقم 06-348 تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق في الجرائم الخطيرة والمعقدة[2] .

وعليه، سيتم تناول هذا المطلب من خلال فرعين؛ نخصص **(الفرع الأول)** لدور القضاء في متابعة الجرائم الرقمية، بينما نخصص **(الفرع الثاني)** لتعزيز فعالية التحقيق والإثبات.

الفرع الأول: دور القضاء في متابعة الجرائم الرقمية

يلعب القضاء دوراً محورياً في مواجهة جرائم العملات الرقمية، لأنه الجهة التي تمنح المواجهة القانونية فعاليتها العملية، من خلال تقدير الوقائع، تكييف السلوك الإجرامي، توجيه الاتهام، الإشراف على التحقيق، والفصل في النزاع. وتزداد أهمية هذا الدور عندما يتعلق الأمر بجرائم العملات الرقمية، لأنها قد

1-المادة 2 من قانون رقم 09-04 مؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، الصادر بتاريخ 16 غشت 2009.

2-المادة الأولى منالمرسوم التنفيذي رقم 06-348 مؤرخ في 12 رمضان عام 1427 الموافق 5 أكتوبر سنة 2006، يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، الجريدة الرسمية للجمهورية الجزائرية، العدد 63، الصادر بتاريخ 8 أكتوبر 2006،

تتداخل مع جرائم متعددة، مثل النصب الإلكتروني، تبييض الأموال، تمويل الإرهاب، اختراق الأنظمة المعلوماتية، وسرقة البيانات أو المحافظ الرقمية.

أولاً: توسيع الاختصاص القضائي لمواجهة الجرائم الرقمية المعقدة

أدرك المشرع الجزائري أن الجرائم الحديثة، ومنها الجرائم المرتبطة بالبيئة الرقمية، لا يمكن مواجهتها دائماً وفق قواعد الاختصاص المحلي التقليدية، لأنها غالباً ما تتجاوز حدود دائرة قضائية واحدة. فقد يقع فعل الاختراق في ولاية، وتتم عملية تحويل الأصول الرقمية في ولاية ثانية، وتستعمل منصة أجنبية أو محفظة إلكترونية خارج الجزائر، مما يجعل توزيع الاختصاص وفق القواعد العادية غير كافٍ لتحقيق نجاعة المتابعة.

ولهذا تم استحداث الأقطاب الجزائية ذات الاختصاص الموسع بموجب القانون رقم 04-14 المعدل والمتمم لقانون الإجراءات الجزائية، ثم جاء المرسوم التنفيذي رقم 06-348 ليحدد كيفية تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق. ويشمل هذا التمديد جرائم ذات طبيعة خطيرة ومعقدة، منها الجريمة المنظمة العابرة للحدود، تبييض الأموال، تمويل الإرهاب، والاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات.[1]

وتظهر أهمية هذه الأقطاب في جرائم العملات الرقمية من حيث إن هذه الجرائم لا تكون دائماً مستقلة بذاتها، بل قد تكون أداة لتنفيذ جرائم أخرى، كأن تُستعمل العملات الرقمية في غسل عائدات الاتجار بالمخدرات، أو تحويل أموال الاحتيال الإلكتروني، أو تمويل نشاط محظور. ولذلك فإن توسيع الاختصاص القضائي يسمح بتجميع عناصر الملف أمام جهة قضائية أكثر قدرة على معالجة القضايا المركبة، بدل تشتيتها بين عدة جهات محلية.

وقد ذهبت بعض الدراسات إلى أن الأقطاب الجزائية المتخصصة تشكل آلية مهمة لمواجهة الجرائم الإلكترونية، بالنظر إلى ما تتيحه من تركيز للاختصاص وتطوير للخبرة القضائية في الجرائم التقنية والمعقدة.[2]

---

1 القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية، العدد 71، الصادرة بتاريخ 10 نوفمبر 2004؛ المرسوم التنفيذي رقم 06-348 المؤرخ في 5 أكتوبر 2006، المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، الجريدة الرسمية للجمهورية الجزائرية، العدد 63، الصادرة بتاريخ 8 أكتوبر 2006.

2 ليندة بومحراث، "مرجع سابق، ص. 6-7.

ثانياً: القطب الجزائي الوطني المتخصص في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

إلى جانب الأقطاب الجزائية ذات الاختصاص الموسع، استحدث المشرع الجزائري القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بموجب الأمر رقم 21-11 المؤرخ في 25 أوت 2021، المعدل والمتمم لقانون الإجراءات الجزائية. ويُعد هذا القطب خطوة مهمة في بناء قضاء متخصص في الجريمة الرقمية، لأن اختصاصه يمتد إلى كامل التراب الوطني، بما يتلاءم مع طبيعة الجريمة الإلكترونية التي لا تخضع للحدود الجغرافية التقليدية.

ويتميز هذا القطب بكونه موجهاً لمعالجة الجرائم المعلوماتية ذات الطابع المعقد، ولا سيما تلك التي يصعب حصر آثارها في مكان واحد. فجرائم العملات الرقمية، بحكم ارتباطها بالمنصات الإلكترونية والمحافظ الرقمية والتحويلات المشفرة، قد تتطلب تدخلاً قضائياً موحداً قادراً على تنسيق التحقيق وتفادي تضارب الإجراءات بين الجهات القضائية المختلفة.

وتتجلى أهمية القطب الجزائي الوطني في ثلاث نقاط أساسية: الأولى أنه يكرس فكرة التخصص القضائي في الجرائم الرقمية؛ والثانية أنه يمنح سلطة متابعة وتحقيق أكثر ملاءمة للجرائم العابرة للاختصاص المحلي؛ والثالثة أنه يسهم في توحيد التكييف القضائي لهذه الجرائم، خصوصاً أن جرائم العملات الرقمية قد تتردد بين عدة أوصاف قانونية، مثل الاحتيال، المساس بأنظمة المعالجة الآلية للمعطيات، تبييض الأموال، أو مخالفة النصوص المتعلقة بحظر التعامل بالعملات الافتراضية.

وقد اعتبرت الدراسات الجامعية الحديثة أن القطب الجزائي الوطني المتخصص يمثل استجابة تشريعية لخصوصية الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، خاصة من حيث تعقيد وسائل ارتكابها وتعدد أماكن تنفيذها وآثارها.[1]

ثالثاً: دور النيابة العامة وقاضي التحقيق في تحريك الدعوى وتوجيه التحقيق

تتولى النيابة العامة دوراً أساسياً في تحريك الدعوى العمومية ومتابعة الجرائم الرقمية، إذ تقوم بتلقي الشكاوى والبلاغات، توجيه الضبطية القضائية، طلب الخبرة الفنية، والإشراف على جمع الأدلة الأولية. وفي جرائم العملات الرقمية، تظهر أهمية النيابة العامة في سرعة التدخل، لأن التأخر في فتح التحقيق قد يؤدي إلى نقل الأصول الرقمية إلى محافظ متعددة أو تحويلها إلى عملات أخرى أو منصات أجنبية.

1 بناصر إنصاف، وعمارة ماضي مراد، القطب الجزائي الوطني المتخصص في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، مذكرة ماستر، تخصص قانون أعمال، 2023-2024كلية الحقوق والعلوم السياسية، جامعة 8 ماي 1945 قالمة،ص. 34.

أما قاضي التحقيق، فيؤدي دوراً أكثر عمقاً في القضايا المعقدة، من خلال الأمر بالتفتيش، الحجز، الخبرة، تتبع الحسابات والبيانات، وسماع الأطراف والشهود والخبراء. وتزداد أهمية التحقيق القضائي في جرائم العملات الرقمية لأن الدليل لا يكون غالباً في حيازة الضحية فقط، بل قد يوجد لدى مزودي خدمات الإنترنت، منصات التداول، البنوك، أو داخل أجهزة إلكترونية تحتاج إلى فحص تقني متخصص.

ومن ثم، فإن فعالية القضاء في هذه الجرائم لا تقاس فقط بقدرته على إصدار الأحكام، بل بقدرته على إدارة التحقيق الرقمي إدارة دقيقة تحفظ الدليل، وتربط بين المعاملة الرقمية والشخص المسؤول عنها، وتمنع ضياع القرائن التقنية التي قد تكون حاسمة في الإدانة أو البراءة

الفرع الثاني: تعزيز فعالية التحقيق والإثبات

تمثل مرحلة التحقيق والإثبات جوهر المواجهة القضائية لجرائم العملات الرقمية، لأن هذه الجرائم لا تُثبت غالباً بالأدلة التقليدية وحدها، بل تحتاج إلى دليل رقمي قابل للفحص والتحقق. ويشمل ذلك سجلات الدخول، عناوين المحافظ، بيانات التحويلات، عناوين بروتوكول الإنترنت، أجهزة الحاسوب والهواتف، رسائل التصيد، والملفات الخبيثة المستعملة في الاختراق أو الاحتيال.

أولاً: استعمال إجراءات البحث والتحري الخاصة

أقر المشرع الجزائري، بموجب القانون رقم 09-04، مجموعة من الإجراءات الخاصة التي تهدف إلى تمكين السلطات المختصة من مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال. ومن أبرز هذه الإجراءات مراقبة الاتصالات الإلكترونية، تفتيش المنظومات المعلوماتية، حجز المعطيات، وحفظ المعلومات التي قد تكون مفيدة في كشف الجرائم أو مرتكبيها. وينص القانون رسمياً على إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مع تحديد مهامها في الوقاية والمساعدة على التحريات وتبادل المعلومات .

وتُعد هذه الإجراءات ذات أهمية خاصة في جرائم العملات الرقمية، لأن الجاني قد يستعمل عدة وسائل لإخفاء أثره، مثل الشبكات الخاصة الافتراضية، المحافظ غير الموثقة، المنصات الأجنبية، أو تقسيم التحويلات بين عدة عناوين. لذلك، فإن التحقيق في هذه الجرائم يحتاج إلى أدوات قانونية تسمح

بالوصول إلى البيانات التقنية، مع احترام الضمانات الدستورية والقانونية المتعلقة بالخصوصية وسرية المراسلات.[1]

ويجب التنبيه هنا إلى أن اللجوء إلى هذه الإجراءات لا يكون بصورة مطلقة، بل ينبغي أن يتم وفق ضوابط قانونية وتحت رقابة القضاء، لأن مكافحة الجريمة الرقمية لا تبرر إهدار الحقوق والحريات الأساسية. فالمعادلة الدقيقة في هذا المجال تقوم على تمكين القاضي والمحقق من كشف الجريمة، دون تحويل أدوات التحري الرقمية إلى وسائل انتهاك غير مشروع للخصوصية[2].

ثانياً: حفظ الدليل الرقمي وسلسلة الحيازة

تُعد مسألة حفظ الدليل الرقمي من أكثر المسائل حساسية في جرائم العملات الرقمية، لأن الدليل الإلكتروني قابل للتغيير أو الحذف أو التلف بسهولة. فقد يكون الدليل عبارة عن ملف في جهاز الضحية، أو سجل دخول إلى منصة، أو رسالة بريد إلكتروني احتيالية، أو عنوان محفظة استقبل أموالاً مسروقة. وإذا لم يتم حفظ هذا الدليل بطريقة سليمة، فقد يفقد قيمته أمام القضاء.

ومن الناحية العملية، يجب أن يتم جمع الدليل الرقمي وفق ما يعرف بسلسلة الحيازة، أي توثيق كل مرحلة يمر بها الدليل منذ ضبطه إلى غاية عرضه أمام المحكمة. ويشمل ذلك تحديد الجهة التي جمعته، تاريخ وساعة الجمع، طريقة النسخ أو الحجز، وسلامة الوسيط الإلكتروني الذي حُفظ عليه. وتظهر أهمية هذا الإجراء في منع الدفع بتغيير الدليل أو العبث به.

وفي جرائم العملات الرقمية، يضاف إلى ذلك ضرورة توثيق مسار الأموال على سلسلة الكتل، من خلال تحديد عنوان المحفظة المرسلة، عنوان المحفظة المستقبلة، تاريخ العملية، قيمتها، ورقم المعاملة. غير أن إثبات انتقال العملة من عنوان إلى آخر لا يكفي وحده لإثبات هوية الجاني، لأن عنوان المحفظة لا يكشف بذاته عن الشخص الطبيعي الذي يستعمله. لذلك لا بد من الربط بين التحليل التقني والمعطيات الشخصية أو المصرفية أو الاتصالية المتاحة في الملف.

ثالثاً: الخبرة القضائية الرقمية ودورها في فهم المعطيات التقنية

[1]-بناصر إنصاف، وعمارة ماضي مراد،مرجع سابق ص 36.

2 المواد من 10الى 14 من قانون رقم 09-04 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، الصادرة بتاريخ 16 أوت 2009.

تفرض جرائم العملات الرقمية على القضاء الاستعانة بالخبرة الفنية، لأن القاضي لا يستطيع في الغالب أن يفصل في المسائل التقنية الدقيقة دون مساعدة مختصين. فالخبير الرقمي يساعد في فحص الأجهزة، استخراج البيانات، تحليل البرمجيات الخبيثة، تتبع المعاملات على البلوكشين، وبيان ما إذا كان الدخول إلى النظام قد تم بطريقة مشروعة أو غير مشروعة.

وتزداد أهمية الخبرة عندما يتعلق الأمر بإثبات العلاقة بين الفعل والنتيجة؛ كأن يثبت الخبير أن رسالة تصيد أدت إلى تسريب بيانات المحفظة، أو أن برنامجاً خبيثاً استُعمل لسرقة المفاتيح الخاصة، أو أن الأموال المسروقة حُولت إلى عنوان معين ثم إلى منصة تداول محددة. وفي هذه الحالة، لا يكون دور الخبير بديلاً عن دور القاضي، وإنما هو وسيلة فنية تساعد القاضي على تكوين اقتناعه.

وقد أشار القانون رقم 09-04 إلى إمكانية تقديم الدعم للسلطات القضائية ومصالح الضبطية القضائية في تحرياتها، بما يشمل تجميع المعلومات وإنجاز الخبرات القضائية اللازمة. وتؤكد الدراسات المتعلقة بالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال أن من مهامها مساعدة السلطات القضائية في التحريات ذات الطابع التقني.[1]

رابعاً: التعاون بين القضاء والضبطية القضائية ومقدمي الخدمات

لا يمكن للقضاء أن يواجه جرائم العملات الرقمية بمعزل عن باقي الفاعلين، لأن جزءاً مهماً من الأدلة يكون في حيازة جهات تقنية أو تجارية، مثل مزودي خدمات الإنترنت، منصات التداول، شركات الاتصالات، البنوك، أو الجهات المكلفة بحماية البيانات والمعطيات. لذلك، فإن التنسيق بين القضاء والضبطية القضائية ومقدمي الخدمات يمثل ركناً أساسياً في فعالية التحقيق.

وقد ألزم القانون رقم 09-04 مقدمي الخدمات بمساعدة السلطات في جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات، مع حفظها ووضعها تحت تصرف الجهات القضائية المختصة وفق الشروط القانونية. كما نص على إجراءات تتعلق بسحب المحتويات غير المشروعة أو جعل الدخول إليها غير ممكن عند الاقتضاء.[2]

1 بوكري أسماء، وصالحي أمينة، المركز الوطني للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مذكرة ماستر، جامعة جيجل، كلية الحقوق والعلوم السياسية، قسم الحقوق، تخصص قانون أعمال، 2020-2021، ص. 35.

2القانون رقم 09-04المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

وتبرز أهمية هذا التعاون في جرائم العملات الرقمية عندما يحتاج القاضي أو المحقق إلى معرفة صاحب عنوان إلكتروني، أو تحديد الجهاز المستعمل في الدخول إلى منصة، أو تتبع حساب استُخدم في شراء أصول رقمية، أو ربط تحويل مشبوه ببيانات تعريفية موجودة لدى مؤسسة مالية أو مزود خدمة. وكلما كان التعاون سريعاً ومنظماً، زادت فرص حفظ الدليل ومنع الجاني من إخفاء أثره.

خامساً: التكوين القضائي المتخصص في الجريمة الرقمية

إن فعالية التحقيق والإثبات لا تتوقف على وجود النصوص القانونية فقط، بل تتطلب تكويناً متخصصاً للقضاة وأعضاء النيابة العامة وضباط الشرطة القضائية. فجرائم العملات الرقمية تقوم على مفاهيم تقنية مثل المفاتيح الخاصة، المحافظ الباردة والساخنة، البلوكشين، العناوين الرقمية، ومنصات التداول، وهي مفاهيم يجب فهمها حتى يتم تكييف الوقائع تكييفاً صحيحاً.

وقد أشار ما ورد في المادة التي أرسلتها إلى أن المصلحة المركزية لمكافحة الجريمة السيبرانية تنسق مع جهاز العدالة، وتباشر مهامها تحت إشراف السلطات القضائية، كما تساهم في تكوين تقني أساسي لفائدة الطلبة القضاة وفق اتفاقية بين وزارة العدل والمديرية العامة للأمن الوطني. وتُعد هذه الخطوة مهمة لأنها تقلل الفجوة بين النص القانوني والواقع التقني للجريمة.[1]

وبناءً على ذلك، فإن تعزيز فعالية التحقيق والإثبات في جرائم العملات الرقمية لا يتحقق إلا بتحديث المعرفة القضائية، وتطوير الخبرة الرقمية، وتوفير أدوات تحليل متخصصة، حتى لا تبقى النصوص القانونية عاجزة أمام تطور الأساليب الإجرامية.

المطلب الثالث: التحديات التقنية وسبل تطويرها

يثير التعامل بالعملات المشفرة مجموعة من الإشكالات المعقدة التي لا تقف عند حدود الجانب الاقتصادي أو المالي، بل تمتد إلى المجالين القانوني والأمني، بالنظر إلى الطبيعة اللامادية لهذه الأصول واعتمادها على تقنيات تشفير متقدمة. وقد أفرز هذا الواقع صعوبات جدية أمام أجهزة إنفاذ القانون، خصوصاً في ما يتعلق بتتبع الجرائم، تحديد هوية مرتكبيها، حجز العائدات الإجرامية، وإثبات العلاقة بين الجاني والمعاملة الرقمية محل الاشتباه.

1 العون الشبيه غنية حساني، "SCLC... العصب الرقمي لصد الجرائم المعلوماتية"، مجلة الشرطة، العدد 158، ماي 2024، ص. 19-20.

وأمام هذه التحديات، لم يعد من الممكن الاكتفاء بالوسائل التقليدية في مكافحة الجريمة، بل أصبح من الضروري تطوير التشريعات، وتحديث آليات التحقيق، وتعزيز قدرات القضاء والضبطية القضائية، إلى جانب تبني حلول وقائية قادرة على مواكبة سرعة تطور البيئة الرقمية. وعليه، سيتم تناول هذا المطلب من خلال فرعين؛ يُخصص(**الفرع الأول**) لبيان التحديات التقنية والقانونية، بينما يُخصص(**الفرع الثاني**) لدراسة سبل تطوير التشريعات والحلول الوقائية.

الفرع الأول: التحديات التقنية والقانونية

تتجسد أولى التحديات التقنية المرتبطة بجرائم العملات المشفرة في غياب السلطة المركزية المتحكمة في هذه الأصول. فبخلاف الأصول المالية التقليدية التي تمر عبر البنوك والمؤسسات المالية الخاضعة للرقابة، تقوم العملات المشفرة، وعلى رأسها البيتكوين، على تقنية **سلاسل الكتل(Blockchain)**، التي تعمل وفق نظام لامركزي لا يخضع لإدارة أو سلطة واحدة.

ويترتب على هذه اللامركزية أثر قانوني بالغ الأهمية، يتمثل في صعوبة استعمال الآليات التقليدية للحجز أو التجميد. ففي النظام المصرفي العادي يمكن للجهات القضائية أن تأمر البنك بتجميد الحساب أو حجز الرصيد، أما في العملات المشفرة فلا يوجد وسيط مالي مركزي يمكن إلزامه بتنفيذ هذا الأمر. ولذلك لا يكون الحجز فعالاً إلا إذا تمكنت الضبطية القضائية أو الجهة القضائية من الوصول إلى **المفاتيح الخاصة(Private Keys)**التي تخول لصاحبها التصرف في الأصول الرقمية.[1]

ولا يقل تحدي إخفاء الهوية خطورة عن تحدي اللامركزية. فرغم أن معاملات العملات المشفرة تكون مسجلة علناً على سلسلة الكتل، إلا أن هذه المعاملات لا ترتبط عادةً بأسماء وهوّيات حقيقية، وإنما بعناوين رقمية مشفرة. وهذا الوضع يمنح الجناة هامشاً واسعاً لإخفاء شخصياتهم، وتحويل عائدات الجريمة، وغسل الأموال بعيداً عن أنظمة الإخطار التي تلتزم بها المؤسسات المالية التقليدية.[2]

وتزداد الصعوبة التقنية عندما يتعلق الأمر بإخفاء الأدلة أو إتلافها. فالعملات المشفرة لا تشغل حيزاً مادياً يمكن ضبطه بسهولة، بل قد تُخزن مفاتيحها في أجهزة صغيرة مثل وحدات التخزين (USB)،

1 مناصرة يوسف، "حجز العملات الافتراضية للضبطية القضائية والقضاة"، مجلة صوت القانون، المجلد 12، العدد 01، 2025، ص. 447.

2 بن معتوق صابر، "تحديات التعامل بالعملات المشفرة – البتكوين نموذجاً"، المجلة الجزائرية للأبحاث الاقتصادية والمالية، المجلد 3، العدد 2، 2020، ص. 105.

أو في محافظ رقمية، أو حتى في خدمات تخزين سحابي. كما يمكن للمشتبه فيه، خلال وقت قصير، أن يمسح محفظته الرقمية، أو يعيد تهيئة جهازه الإلكتروني، أو يتلف المعطيات ذات الصلة، بما يؤدي إلى ضياع الدليل الجنائي أو صعوبة استرجاعه.[1]

أما على المستوى القانوني والمؤسساتي، فإن مواجهة هذه الجرائم تصطدم بمحدودية قدرة الهياكل القضائية التقليدية على التعامل مع جرائم ذات طبيعة تقنية عالية. وقد عبّر الفقه عن هذه الصعوبة من خلال التأكيد على: «عجز الجهاز القضائي العادي عن مكافحة الجريمة المنظمة في ظل غياب الوسائل التشريعية والتنظيمية التي يمكنها استيعاب أشكال الجريمة المنظمة في العصر الحالي المرتبطة بوسائل الاتصال الحديثة».[2]

وتظهر أهمية هذا الطرح في أن جرائم العملات المشفرة لا تتطلب فقط معرفة بالنصوص القانونية، بل تستدعي فهماً دقيقاً لتقنيات التشفير، المحافظ الرقمية، سلاسل الكتل، منصات التداول، وآليات إخفاء الهوية. لذلك فإن قاضي التحقيق أو جهة الحكم التي لا تمتلك دعماً فنياً متخصصاً قد تواجه صعوبة في تكييف الوقائع أو تقدير الأدلة الرقمية تقديراً سليماً.[3]

ويضاف إلى ذلك تحدٍ آخر يتمثل في ضعف الاعتراف الدولي الموحد بالعملات المشفرة.
فالتشريعات المقارنة لا تتبنى موقفاً واحداً تجاه هذه العملات؛ إذ تتجه بعض الدول إلى الحظر، بينما تختار دول أخرى التنظيم أو الاعتراف الجزئي. ويؤدي هذا التباين إلى خلق فراغات قانونية يستغلها الجناة، خاصة في الجرائم العابرة للحدود، حيث يمكن تحويل الأصول الرقمية إلى منصات أو ولايات قضائية أقل صرامة.[4]

وعليه، فإن التحديات التقنية والقانونية المرتبطة بجرائم العملات المشفرة لا تنحصر في صعوبة كشف الجريمة، بل تمتد إلى صعوبة الحجز، التجميد، الإثبات، تحديد المسؤولية، وتجاوز التنازع بين الأنظمة القانونية المختلفة.

الفرع الثاني: تطوير التشريعات والحلول الوقائية

1 مناصرة يوسف، "حجز العملات الافتراضية"، ص. 459.

2 ليندة بومحراث، مرجع سبق ذكره ، ص. 11.

3 المرجع نفسه، ص. 10-11.

4 بن معتوق صابر،المرجع السابق، ص. 104.

أمام الطبيعة المعقدة لجرائم العملات المشفرة، يصبح تطوير التشريعات والحلول الوقائية ضرورة لا مجرد خيار. فالمواجهة الفعالة لا تتحقق من خلال التجريم وحده، بل تستلزم بناء منظومة متكاملة تجمع بين التخصص القضائي، التحديث التنظيمي، تطوير قدرات التحقيق الرقمي، وتعزيز التعاون بين المؤسسات الوطنية والدولية.

أولاً: دعم القضاء المتخصص

يُعد التوجه نحو القضاء المتخصص من أهم الحلول المؤسساتية لمواجهة جرائم العملات المشفرة. فقد أثبتت التجربة أن الجرائم الرقمية لا يمكن أن تُعالج دائماً بنفس الآليات المطبقة على الجرائم التقليدية، لأنها تتطلب خبرة فنية وقانونية متداخلة. ومن هنا تبرز أهمية استحداث الأقطاب الجزائية المتخصصة، باعتبارها جهات قضائية ذات اختصاص إقليمي موسع، قادرة على معالجة الجرائم المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

ويظهر دور هذه الأقطاب في أنها تسمح بتركيز الخبرة القضائية، وتسهيل التنسيق بين قضاة التحقيق والنيابة والضبطية القضائية، وتطوير أساليب البحث والتحري الخاصة بالجرائم التقنية. كما أنها تتيح معالجة أكثر فعالية للجرائم التي تتجاوز حدود الاختصاص المحلي التقليدي، وهو أمر يتناسب مع طبيعة جرائم العملات المشفرة التي قد تمتد آثارها إلى أكثر من إقليم أو دولة.[1]

ثانياً: تحديث الأطر التنظيمية والرقابية

لا يكفي استحداث قضاء متخصص إذا لم ترافقه أطر تنظيمية مرنة قادرة على مواكبة التطورات التقنية. وفي هذا السياق، دعت الهيئات المالية الدولية إلى تكييف القواعد التنظيمية والرقابية مع التحولات التي فرضتها التكنولوجيا المالية. وقد تجلى ذلك في **أجندة مؤتمر بالي للتكنولوجيا المالية** لسنة 2018، التي أكدت ضرورة: «تكييف الإطار التنظيمي والممارسات الإشرافية وذلك من أجل تطوير واستقرار النظام المالي على نحو منتظم... وتدعيم الثقة والاطمئنان والاستجابة للمخاطر».[2]

1ليندة بومحراث، "الأقطاب الجزائية المتخصصة"، ص. 10-11.

2 ن معتوق صابر، المرجع السابق، ص. 106.

ويفهم من ذلك أن التعامل مع العملات المشفرة لا ينبغي أن يقوم فقط على المنع أو الردع، بل يجب أن يستند إلى سياسة تنظيمية قادرة على حماية النظام المالي، وتعزيز الامتثال لتدابير مكافحة غسل الأموال وتمويل الإرهاب، وتوسيع نطاق المراقبة الجماعية للنظام المالي الدولي.[1]

1 المرجع نفسه، ص. 106.

ثالثاً: تكوين الأجهزة القضائية والأمنية في تحليل سلاسل الكتل

تتطلب جرائم العملات المشفرة تكويناً مستمراً للقضاة، وأعضاء النيابة، وضباط الشرطة القضائية، والخبراء، خاصة في مجال تحليل سلاسل الكتل وتتبع التدفقات الرقمية. فالمعاملة الرقمية قد تكون ظاهرة على السلسلة، غير أن الربط بينها وبين الشخص الطبيعي أو المعنوي الذي يقف وراءها يحتاج إلى مهارات فنية متخصصة.

ويشمل هذا التكوين فهم آليات إنشاء المحافظ، طبيعة المفاتيح الخاصة، طرق إخفاء الهوية، وسائل تحليل المعاملات، مؤشرات الاشتباه، وكيفية الحفاظ على الدليل الرقمي. كما يستلزم الأمر توفير أدوات تقنية تساعد جهات التحقيق على تتبع حركة الأصول الرقمية بين المحافظ والمنصات، خاصة عندما يحاول الجاني نقلها بسرعة أو تقسيمها لإخفاء مصدرها.

رابعاً: تعزيز التعاون بين القطاعين العام والخاص

من بين الحلول الوقائية المهمة بناء قنوات تعاون فعالة بين السلطات العامة ومزودي خدمات الأصول الافتراضية (**VASPs**) .فهذه الجهات تمتلك في كثير من الأحيان معلومات تقنية وبيانات تعامل قد تكون حاسمة في كشف الجريمة، مثل بيانات فتح الحساب، سجلات الدخول، عناوين المحافظ، والتحويلات المنفذة عبر المنصة.

ويقتضي هذا التعاون وضع قواعد واضحة لتبادل المعلومات الفنية والتكتيكية بين سلطات إنفاذ القانون والقطاع الخاص، مع احترام الضمانات القانونية المتعلقة بالخصوصية وحماية البيانات. كما يجب إلزام مزودي الخدمات بالاحتفاظ بالبيانات، والتبليغ عن العمليات المشبوهة، وتنفيذ أوامر التجميد أو الحجز متى كان ذلك ممكناً قانوناً وتقنياً[1].

خامساً: توحيد المعايير الدولية وتعزيز التعاون العابر للحدود

نظراً للطبيعة العابرة للحدود لجرائم العملات المشفرة، فإن تطوير التشريعات الوطنية يظل محدود الأثر إذا لم يواكبه تنسيق دولي فعال. فالجاني قد يوجد في دولة، والمنصة في دولة ثانية، والضحية في دولة ثالثة، بينما تمر الأموال عبر محافظ متعددة يصعب ربطها باختصاص قضائي واحد.

[1]-لينده بومحراث، مرجع سابق، ص15.

لذلك تبرز الحاجة إلى وضع معايير تنظيمية دولية موحدة، تقلل من الفجوات القانونية التي يستغلها المجرمون. كما ينبغي تعزيز آليات المساعدة القانونية المتبادلة، وتفعيل التعاون عبر المنظمات الدولية، مثل الإنتربول واليوروبول، بما يضمن سرعة تبادل المعلومات واسترداد العائدات الإجرامية العابرة للحدود.[1]

وبناءً على ذلك، فإن الحلول الوقائية لا تقتصر على الجانب التقني، بل تشمل إصلاحاً تشريعياً ومؤسساتياً متكاملاً، يقوم على التخصص، التكوين، التنظيم، التعاون، وتوحيد المعايير، حتى تتمكن الدولة من مواجهة جرائم العملات المشفرة بفعالية أكبر.

1 مناصرة يوسف، مرجع سبق ذكره، ص. 460.

خلاصة الفصل

نخلص من خلال دراسة هذا الفصل إلى أن الطبيعة اللامادية واللامركزية للعملات الرقمية قد أحدثت هوة عميقة بين دهاء الأساليب الإجرامية وقدرة القواعد التقليدية على الردع. لقد كشفت الدراسة التطبيقية أن العملات المشفرة، رغم فوائدها التقنية، أضحت المحرك الأساسي للعديد من الجرائم السيبرانية والاقتصادية، لاسيما في مجالات غسل الأموال والتهرب الضريبي. إن غياب الكيان المركزي الذي يتحكم في هذه الأصول يجعل من عمليات التجميد أو المصادرة التقليدية أمراً مستحيلاً، مما يستوجب الانتقال نحو استراتيجيات تقنية تعتمد على السيطرة على "المفاتيح الخاصة" وتحليل بيانات "سلاسل الكتل."

كما أظهرت الدراسة أن المشرع الجزائري، من خلال استحداثه للأقطاب الجزائية المتخصصة، قد خطا خطوة جادة نحو إرساء نظام قضاء متخصص قادر على استيعاب تعقيدات الإجرام المعلوماتي. ومع ذلك، فإن الواقع العملي أثبت أن النصوص القانونية وحدها تبقى قاصرة ما لم ترفق بتعاون دولي وثيق وتدريب تقني عالي المستوى لضباط الشرطة القضائية والقضاة، نظراً لقدرة الجناة على تدمير الأدلة الرقمية بسرعة فائقة. إن ختام هذه الدراسة يضعنا أمام حتمية المزاوجة بين "قوة النص القانوني" و"كفاءة الأدوات التقنية" لضمان بيئة رقمية آمنة ومستقرة.

خـــاتـــمـــة

خاتمة

من خلال هذه الدراسة، يتضح أن العملات الرقمية لم تعد مجرد ظاهرة تقنية أو مالية حديثة، بل أصبحت واقعاً قانونياً وأمنياً يفرض نفسه على التشريعات الوطنية والأنظمة القضائية. فقد كشفت الدراسة أن هذه العملات تتميز بطبيعة خاصة تقوم على اللامركزية، والتشفير، وغياب الوسيط، والطابع العابر للحدود، وهي خصائص جعلتها وسيلة سريعة ومبتكرة في المعاملات الرقمية، لكنها في الوقت نفسه وفرت بيئة ملائمة لارتكاب أنماط جديدة من الجرائم، خاصة الاحتيال الرقمي، غسل الأموال، تمويل الأنشطة غير المشروعة، واختراق المحافظ الرقمية.

تخضع الجرائم الناشئة عن التعامل بالعملات المشفرة، في أصلها الجنائي، لذات الضوابط والأحكام العامة التي تحكم الجريمة التقليدية؛ إذ لا يمكن مساءلة الجاني أو توقيع العقاب عليه في البيئة الرقمية إلا إذا تضافرت ثلاثة أركان أساسية تمنح الفعل صفته غير المشروعة.

ويأتي في طليعة هذه الأركان الركن الشرعي، الذي يُمثّل الحصانة القانونية للأفراد تجسيداً لمبدأ "لا جريمة ولا عقوبة إلا بنص"؛ فلا يمكن تجريم أي سلوك مرتبط بالأصول الافتراضية ما لم يكن المشرع قد نص صراحةً على حظره أو منعه بموجب النصوص العقابية الموضوعية أو القوانين الخاصة المتصلة بتقنيات الإعلام والاتصال.

أما المظهر الملموس الذي يخرج به هذا السلوك إلى العالم الخارجي فيتجسد في الركن المادي، وهو القوام التنفيذي للجريمة الذي لا يقوم بدونه اعتداء؛ ويتمثل في البيئة الرقمية في صور شتى كالاحتيال، أو اختراق المحافظ الإلكترونية، أو توجيه المعاملات المشفرة لغسل الأموال وتمويل الإرهاب، حيث ترتبط فيه النتيجة الإجرامية بالسلوك عبر رابطة سببية تقنية ومعقدة، تفرض تحديات جمة في إثباتها نظراً لخصائص التشفير واللامركزية.

وأخيراً، يتكامل هذا البناء القانوني بـ الركن المعنوي، الذي يمثل الجانب النفسي والداخلي للجاني؛ إذ يشترط القانون قيام القصد الجنائي بعنصريه "العلم والإرادة"، بحيث يكون المتهم على علم تام بالطبيعة غير المشروعة لفعله، وتتجه إرادته الحرة والواعية نحو تطويع المزايا التقنية للعملات الرقمية لتحقيق النتيجة الإجرامية المبتغاة، مع رغبته في التخفي وراء الهوية الرقمية للإفلات من يد العدالة.

كما تبين أن الإشكال لا يكمن فقط في وجود هذه العملات، وإنما في صعوبة إخضاعها للقواعد القانونية التقليدية، سواء من حيث التكييف القانوني، أو تحديد المسؤولية الجنائية، أو إثبات الجريمة، أو تحديد الجهة القضائية المختصة. وقد أظهرت المعالجة أن المشرع الجزائري اتجه إلى الحذر والحظر في

التعامل مع العملات الافتراضية، مع الاعتماد على نصوص متفرقة في قانون العقوبات، وقانون الوقاية من تبييض الأموال وتمويل الإرهاب، والقانون رقم 09-04 المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، إضافة إلى آليات القضاء المتخصص لمواجهة الجرائم الرقمية المعقدة. وهذا ينسجم مع ما انتهت إليه الدراسة في الفصل الأول من أن العملات الرقمية تخلق تحديات حقيقية في الإثبات والاختصاص، ومع ما عالجه الفصل الثاني من صور الجرائم وآليات مكافحتها.

النتائج:

خلصت الدراسة إلى النتائج الآتية:

1. العملات الرقمية تختلف عن النقود الإلكترونية والعملات الافتراضية من حيث الطبيعة القانونية والتقنية، خاصة لارتباطها بالتشفير واللامركزية وغياب الغطاء النقدي التقليدي.

2. الخصائص التقنية للعملات الرقمية، مثل إخفاء الهوية وسرعة التحويل وصعوبة التتبع، جعلتها أكثر قابلية للاستغلال في الأنشطة الإجرامية مقارنة بوسائل الدفع التقليدية.

3. موقف المشرع الجزائري من العملات الافتراضية يغلب عليه الطابع الحظري، خاصة من خلال منع شراء أو بيع أو استعمال أو حيازة العملة الافتراضية، غير أن هذا الحظر لا يكفي وحده لمواجهة الجرائم المرتبطة بها.

4. جرائم العملات الرقمية لا تقتصر على الاحتيال المالي، بل تمتد إلى غسل الأموال، تمويل الإرهاب، سرقة البيانات، اختراق المحافظ الرقمية، واستغلال الأجهزة في التعدين غير المشروع.

5. تطبيق القواعد العامة للمسؤولية الجنائية على جرائم العملات الرقمية يثير صعوبات عملية، خصوصاً في تحديد الركن المادي للجريمة وربطه بالفاعل الحقيقي في بيئة رقمية مجهولة أو مستعارة.

6. الدليل الإلكتروني أصبح محورياً في إثبات جرائم العملات الرقمية، غير أن حجيته تتوقف على سلامة جمعه وحفظه وربطه بالمتهم دون انقطاع في سلسلة الحيازة.

7. قواعد الاختصاص القضائي التقليدية لم تعد كافية لمواجهة جرائم العملات الرقمية، لأنها غالباً ما تقع عبر أكثر من إقليم ودولة ومنصة رقمية.

8. إنشاء الأقطاب الجزائية المتخصصة يمثل خطوة مهمة في مواجهة الجرائم الرقمية، لكنه يحتاج إلى دعم تقني وخبرة متخصصة حتى يكون فعالاً في جرائم العملات المشفرة.

9. مكافحة جرائم العملات الرقمية لا يمكن أن تتم بالوسائل القانونية التقليدية وحدها، بل تتطلب الجمع بين النص القانوني، الخبرة التقنية، التعاون الدولي، وآليات التتبع والتحليل الرقمي.

10. هناك حاجة واضحة إلى تطوير الإطار التشريعي الجزائري بما يميز بين العملات الرقمية الرسمية، مثل الدينار الرقمي المحتمل، والعملات الافتراضية اللامركزية التي قد تُستغل في الجرائم المالية.

الاقتراحات:

بناءً على النتائج السابقة، يمكن تقديم الاقتراحات الآتية:

1. ضرورة وضع إطار قانوني خاص بجرائم العملات الرقمية، يحدد بدقة صور التجريم والعقوبات وآليات المتابعة، بدل الاكتفاء بإسقاط النصوص التقليدية عليها.

2. تعديل النصوص المتعلقة بالعملات الافتراضية بما يوضح الجزاءات المترتبة على مخالفة الحظر، حتى لا يبقى النص القانوني عاماً أو ناقص الفعالية العملية.

3. تعزيز تخصص القضاة ووكلاء الجمهورية وقضاة التحقيق في مجال الجرائم الرقمية، من خلال تكوين مستمر في العملات المشفرة، البلوكشين، المحافظ الرقمية، وأدلة التتبع الإلكتروني.

4. دعم الضبطية القضائية بوحدات تقنية متخصصة وأدوات تحليل رقمية قادرة على تتبع التحويلات المشفرة وربطها بالهويات الحقيقية كلما أمكن ذلك.

5. إنشاء آلية وطنية للتنسيق بين القضاء، الضبطية القضائية، بنك الجزائر، خلية معالجة الاستعلام المالي، ومزودي الخدمات الرقمية، قصد تسريع تبادل المعلومات المتعلقة بالمعاملات المشبوهة.

6. تطوير قواعد حجز ومصادرة الأصول الرقمية، لأن مصادرة العملات المشفرة تختلف تقنياً عن حجز الأموال التقليدية وتتطلب معرفة بالمفاتيح الخاصة والمحافظ الرقمية.

7. تفعيل التعاون الدولي في مجال تبادل الأدلة الرقمية وتتبع المحافظ والمنصات الأجنبية، لأن الطابع العابر للحدود هو من أبرز أسباب صعوبة مكافحة هذه الجرائم.

8. إلزام المنصات الرقمية ومقدمي خدمات الأصول الافتراضية، متى تم الترخيص لهم مستقبلاً، بتطبيق قواعد معرفة الزبون والإبلاغ عن العمليات المشبوهة.

9. نشر الوعي القانوني والتقني لدى المستخدمين حول مخاطر الاحتيال الرقمي، عروض العملات الوهمية، التصيد الإلكتروني، وسرقة المفاتيح الخاصة.

10. تشجيع البحث الأكاديمي والقانوني في مجال العملات الرقمية، لأن سرعة تطور هذه الجرائم تفرض تحديثاً مستمراً للمعرفة القانونية والتقنية.

قائمة المصادر والمراجع

Les Références

قائمة المصادر والمراجع

القسم الأول: المراجع باللغة العربية

01- النصوص القانونية:

أولاً- الاتفاقيات والمعاهدات الدولية:

* اتفاقية بودابست المتعلقة بالجرائم المعلوماتية (Convention on Cybercrime)، مجلس أوروبا، 2001.

ثانياً- التشريع الأساسي:

أ- القوانين:

* القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية، العدد 71.

* القانون رقم 09-04 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47.

* القانون رقم 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، العدد 34.

* القانون رقم 23-01 المؤرخ في 07 فبراير 2023، المعدل والمتمم للقانون رقم 06-05، الجريدة الرسمية للجمهورية الجزائرية، العدد 08.

* القانون رقم 23-05 المؤرخ في 07 مايو 2023، المتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والاتجار غير المشروعين بها، الجريدة الرسمية للجمهورية الجزائرية، العدد 32.

* القانون رقم 25-10 المؤرخ في 24 يوليو 2025، المعدل والمتمم للقانون رقم 05-01 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، الجريدة الرسمية للجمهورية الجزائرية، العدد 48.

ب- الأوامر:

* الأمر رقم 75-58 المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني، المعدل والمتمم.

* الأمر رقم 12-02 المؤرخ في 13 فبراير 2012، المعدل والمتمم للقانون رقم 05-01 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، الجريدة الرسمية للجمهورية الجزائرية، العدد 08.

ج- القوانين والأنظمة المقارنة:

* قوانين وأنظمة تنظيم الأصول الافتراضية المقارنة، كالتشريع الإماراتي والبحريني.

ثالثاً- التشريع التنظيمي:

أ- المراسيم التنفيذية:

* المرسوم التنفيذي رقم 06-348 المؤرخ في 05 أكتوبر 2006، المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، الجريدة الرسمية للجمهورية الجزائرية، العدد 63.

ب- التعليمات:

* تعليمة لجنة تنظيم عمليات البورصة ومراقبتها رقم 24-07 المؤرخة في 21 نوفمبر 2024، المتضمنة تدابير اليقظة الواجبة اتجاه الزبائن في إطار الوقاية من تبييض الأموال وتمويل الإرهاب وتمويل انتشار أسلحة الدمار الشامل.

02- الكتب:

أولاً- الكتب العامة:

* أحسن بوسقيعة، الوجيز في القانون الجزائي العام، الطبعة العاشرة، دار هومة، الجزائر، 2011.

* حمد سفر، مكافحة غسل الأموال في البلدان العربية، اتحاد المصارف العربية، بيروت، لبنان، 2003.

* السيد أحمد عبد الخالق، الآثار الاقتصادية والاجتماعية لتبييض الأموال، دار النهضة العربية، القاهرة، مصر، 1997.

* لعشب علي، الإطار القانوني لمكافحة تبييض الأموال، الطبعة الثانية، ديوان المطبوعات الجامعية، الجزائر، 2009.

* محمود نجيب حسني، شرح قانون العقوبات: القسم العام، الطبعة السادسة، دار النهضة العربية، القاهرة، مصر، 1989.

ثانياً- الكتب الخاصة:

* آمال قارة، الحماية الجزائية للمعلومات في التشريع الجزائري، الطبعة الثانية، دار هومة، الجزائر، 2007.

* عثمان عثمانية، ووداد بن قيراط، اقتصاد العملات المشفرة ومستقبل النقود، المركز العربي للأبحاث ودراسة السياسات، بيروت، لبنان، 2022.

* عبد الفتاح بيومي حجازي، الاختصاص القضائي في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية، مصر، 2007.

* علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، لبنان، 1999.

* علي محمد الخوري، المدفوعات الإلكترونية والعملات الرقمية، مجلس الوحدة الاقتصادية العربية بجامعة الدول العربية، الإمارات العربية المتحدة، 2021.

* فتحي الحموري، وناهد، الأوراق التجارية الإلكترونية، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2010.

* طه مصطفى كمال، ووائل أنور بندق، الأوراق التجارية الإلكترونية ووسائل الدفع الإلكترونية الحديثة، دار الفكر الجامعي، الإسكندرية، مصر، 2010.

* لبيب إبراهيم أحمد السيد، الدفع بالنقود الإلكترونية: الماهية والتنظيم القانوني، دراسة تحليلية مقارنة، دار الجامعة الجديدة، الإسكندرية، مصر، 2009.03-

03- المقالات والدراسات:

* أديتيا نارين، ومارينا موريتي، "تنظيم العملات المشفرة"، مجلة التمويل والتنمية، صندوق النقد الدولي، سبتمبر 2022.

* بن معتوق صابر، "تحديات التعامل بالعملات المشفرة – البتكوين نموذجاً"، المجلة الجزائرية للأبحاث الاقتصادية والمالية، المجلد 03، العدد 02، 2020.

* بودقزدام سامية، ونويس نبيل، "سرقة البيانات الإلكترونية: دراسة تأصيلية مقارنة بين الأحكام الشرعية والقانون الجزائري"، مجلة الدراسات القانونية والاقتصادية، المجلد 08، العدد 02، 2025.

* جلول شرارة، وليلى أسمهان بقبق، "العملات الرقمية للبنوك المركزية: تحديات ومتطلبات الدينار الرقمي الجزائري في ظل القانون النقدي والمصرفي 23-09"، مجلة طبنة للدراسات العلمية الأكاديمية، المركز الجامعي سي الحواس بريكة، المجلد 06، العدد 02، 2023.

* جيدول محمد، وعباس حمزة، "حماية الخصوصية والأمن الرقمي في القانون الجنائي"، مجلة الميدان للعلوم الإنسانية والاجتماعية، المجلد 07، العدد 2026، 2026.

* زكرياء مسعودي، وطاد الزهرة جقريف، "ماهية النقود الإلكترونية"، المجلة الدولية للبحوث القانونية والسياسية، المجلد 02، العدد 03، ديسمبر 2018.

* سمر محمد أحمد علي، "العملات الافتراضية المشفرة: ماهيتها وخصائصها ووضعها القانوني"، مجلة جامعة جنوب الوادي الدولية للدراسات القانونية، العدد الثامن، مصر، 2025.

* عاصم عادل محمد العضايلة، "العملات الرقمية الافتراضية طريق لتمويل الإرهاب"، مجلة جامعة الزيتونة الأردنية للدراسات القانونية، المجلد 01، العدد 01، الأردن، 2020.

* العون الشبيه غنية حساني، " SCLC... العصب الرقمي لصد الجرائم المعلوماتية"، مجلة الشرطة، العدد 158، ماي 2024.

* فريدة حداد، وعبد الحق قريمس، "العملة الافتراضية في القانون الجزائري"، المجلة الجزائرية للعلوم القانونية والسياسية.

* كحيل حياة، "حجية الإثبات الإلكتروني"، مجلة البحوث والدراسات القانونية والسياسية، جامعة البليدة 2، العدد التاسع، الجزائر.

* لافي محمد درادكة، "تحديات مواكبة التنظيم القانوني للتطور التكنولوجي للعمل المالي والمصرفي"، مجلة كلية القانون الكويتية العالمية، ملحق خاص، العدد 03، الجزء الأول، مايو 2018.

* محمد الشافعي، "النقود الإلكترونية: ماهيتها ومخاطرها وتنظيمها القانوني"، مجلة الأمن والقانون، أكاديمية شرطة دبي، العدد 01، 2004.

* مناصرة يوسف، "حجز العملات الافتراضية للضبطية القضائية والقضاة"، مجلة صوت القانون، المجلد 12، العدد 01، 2025.

* منصور علي منصور شطا، "العملات الافتراضية المشفرة وأثرها على مستقبل المعاملات: الواقع وآفاق المستقبل"، مجلة كلية الشريعة والقانون بطنطا، جامعة الأزهر، العدد 37، الجزء الأول، مصر، 2022.

* نذير عبد الرزاق، وحجاب عيسى، "وظائف النقود في الفكر الاقتصادي الإسلامي والاقتصاد الوطني: دراسة مقارنة"، مجلة الحقوق والعلوم الإنسانية للدراسات الاقتصادية، المجلد 07، العدد 02، 2013.

* هواري قعموسي، "تجريم العملة الافتراضية الرقمية بقانون تبييض الأموال رقم 25-10 بالجزائر"، المجلة الجزائرية للحقوق والعلوم السياسية، 2025.

* يُغربي حمزة، وبدروني عيسى، "العملات المشفرة: النشأة والتطور والمخاطر"، مجلة الدراسات الاقتصادية المعاصرة، المجلد 05، العدد 02، 2020.

- المداخلات:

* حبيبة عبدلي، ونور الدين موفق، "تبييض الأموال في البيئة الإلكترونية"، المؤتمر الدولي الافتراضي لمكافحة الفساد في البيئة الإلكترونية، المركز الديمقراطي العربي، برلين، 2021.

* ليندة بومحراث، "الأقطاب الجزائية المتخصصة كآلية لمكافحة الجرائم الإلكترونية"، مداخلة مقدمة في الملتقى الدولي: التكنولوجيات الحديثة والجريمة، كلية الحقوق، جامعة الإخوة منتوري قسنطينة 1، الجزائر، 13 نوفمبر 2022.

* عابد صونية، "العملات الرقمية والاستقرار المالي: المزايا والمخاطر والتحديات"، مداخلة مقدمة في الملتقى الدولي حول العملات الرقمية وتحديات الأمن السيبراني، جامعة طاهري محمد، بشار، الجزائر، 20-21 نوفمبر 2024.

04- الأطاريح والمذكرات:

أولاً- أطاريح الدكتوراه:

* جزول صالح، جريمة تبييض الأموال في القانون الجزائري والشريعة الإسلامية: دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة وهران، السنة الجامعية 2014-2015.

ثانياً- مذكرات الماستر:

* بوكري أسماء، وصالحي أمينة، المركز الوطني للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة جيجل، السنة الجامعية 2020-2021.

* بناصر إنصاف، وعمارة ماضي مراد، القطب الجزائي الوطني المتخصص في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة 08 ماي 1945 قالمة، السنة الجامعية 2023-2024.05-

05- الوثائق الأخرى (التقارير والإحصائيات والجرائد):

مبادئ وتوصيات مجموعة العمل المالي (FATF) الخاصة بمخاطر الأصول الافتراضية، التقرير التوجيهي، 2020.

وزارة الاقتصاد والمالية والإنعاش الفرنسية، وحدة معالجة المعلومات والعمل ضد الدوائر المالية السرية TRACFIN، تقرير الاتجاهات وتحليل مخاطر غسل الأموال وتمويل الإرهاب 2019-2020، باريس، 2020.

CNN بالعربية، "اليونان تُسلم أمريكا مواطناً روسياً متهماً بتبييض الأموال"، 04 أوت 2022.

06- المواقع الالكترونية:

https://www.bank-of-algeria.dz:تصريحات الوزير الأول خلال الندوة حول التحديات المستقبلية للبنوك المركزية بمناسبة الذكرى 60 لتأسيس بنك الجزائر، موقع وكالة الأنباء الجزائرية.

- https://btcacademy.online: أكاديمية البيتكوين العربية، "ما هو كريبتوجاكينجCryptojacking؟"، موقع أكاديمية البيتكوين العربية، منشور بتاريخ 08 مارس 2023.
- https://bitcoinarabic.org/أكاديمية البيتكوين العربية، "احتيال عروض العملات الأولية ICO Scam"، موقع أكاديمية البيتكوين العربية.
- https://ar.beincrypto.com/منصة Rain، "ما هو ICO؟ العرض الأولي للعملة"، موقع Rain، منشور بتاريخ 05 نوفمبر 2025.
- https://www.cryptopolitan.com/ar/، "مخططات بونزي مقابل الهرم: احذر من الخداع"، موقع Cryptopolitan.

القسم الثاني: المراجع باللغة الأجنبية (References / Bibliographie)

1-Books / Ouvrages:

- Alice Ekman, China's Blockchain and Cryptocurrency Ambitions the first mover advantage, European Union Institute for Security Studies (EUISS), 2021.
- Financial Action Task Force (FATF), Virtual Currencies: Key Definitions and Potential AML/CFT Risks, Paris: FATF, 2014.
- FATF, Virtual Assets: Red Flag Indicators of Money Laundering and Terrorist Financing, Paris: FATF/OECD, September 2020.
- FATF, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, Paris: FATF/OECD, October 2021.

2-Articles:

- ALUMASEANU S., Le traitement pénal du Bitcoin et des autres monnaies virtuelles, Gaz. Pal 2014, no 242.

- Fratzscher, M & ،.Mehl, A., China's Dominance Hypothesis and the Emergence of a Tri-polar Global Currency System, The Economic Journal, 124(581), 2014.
- G. MARRAUD des GROTTES, Auditions au Sénat sur la blockchain : les incompréhensions demeurent…, RLDA N°135, 1er mars 2018.
- Haroon Al-Tarawneh, NajwanAbdallat&Mohamad Al-Laham, "Development of Electronic Money and Its Impact on the Central Bank Role and Monetary Policy," Issues in Informing Science and Information Technology 6, 2009.
- Mathis B., Quel régime juridique pour les cryptoactifs, RLDA 2018/143, Suppl., n° 6613.
- Prasad, E., and Ye, L., The RenminbiProspects as a Global Reserve Currency, Cato Journal, 33(3), 2013.

3-Laws / Lois:

- Markets in Crypto-Assets - MiCA.(لائحة الأسواق في الأصول المشفرة الأوروبية)

الـــفـــهـــرس

الفهرس

الملخص

الملخص

ملخص:

تعالج هذه الدراسة موضوع جرائم العملات الرقمية من الناحية القانونية، باعتبارها من الجرائم المستحدثة المرتبطة بالتطور التكنولوجي والمالي. وتهدف إلى بيان ماهية العملات الرقمية وخصائصها وتكييفها القانوني، ثم تحليل الأساس القانوني للمسؤولية الجنائية عنها. كما تتناول أهم صور الجرائم المرتبطة بها، خاصة الاحتيال الرقمي، غسل الأموال، تمويل الأنشطة غير المشروعة، واختراق المحافظ الرقمية. وتخلص الدراسة إلى أن مواجهة هذه الجرائم تتطلب تطوير النصوص القانونية، وتعزيز القضاء المتخصص، واعتماد آليات فعالة للإثبات والتحري الرقمي.

الكلمات المفتاحية :العملات الرقمية، الجرائم الإلكترونية، المسؤولية الجنائية، غسل الأموال، الإثبات الرقمي.

Résumé

Cette étude traite les crimes liés aux monnaies numériques d'un point de vue juridique, en tant que formes récentes de criminalité issues de l'évolution technologique et financière. Elle vise à définir les monnaies numériques, leurs caractéristiques et leur qualification juridique, puis à analyser le fondement de la responsabilité pénale. L'étude aborde également les principales formes criminelles associées, notamment la fraude numérique, le blanchiment d'argent, le financement d'activités illicites et le piratage des portefeuilles numériques. Elle conclut à la nécessité d'adapter les textes juridiques, de renforcer la spécialisation judiciaire et d'améliorer les mécanismes de preuve et d'enquête numériques.

Mots-clés : monnaies numériques, cybercriminalité, responsabilité pénale, blanchimentd'argent, preuve numérique.

Abstract

This study examines crimes related to digital currencies from a legal perspective, as emerging offenses resulting from technological and financial development. It aims to define digital currencies, identify their characteristics and legal classification, and analyze the legal basis of criminal liability. The study also addresses the main forms of crimes associated with digital currencies, including digital fraud, money laundering, financing illicit activities, and hacking digital wallets. It concludes that combating these crimes requires updating legal rules, strengthening specialized judicial bodies, and adopting effective mechanisms for digital investigation and electronic evidence.

Keywords: digital currencies, cybercrime, criminal liability, money laundering, digital evidence.