



Abstract:

The research explores crimes associated with encryption and digital currencies from a legal and criminal perspective. It highlights the nature and diversity of these offenses, such as financial fraud, money laundering, and tax evasion, which have grown more complex with the advancement of digital technologies. The study also addresses the legal challenges faced by legislative and judicial bodies in combating these crimes, especially given the absence of a unified international legal framework and the difficulty of tracking digital transactions.

Furthermore, the research examines how national criminal laws deal with such offenses and assesses whether existing legal provisions are sufficient to deter perpetrators. It emphasizes the need to develop new laws that align with the digital nature of these crimes. The study also underscores the importance of international cooperation in strengthening criminal accountability through information exchange, coordinated efforts among countries, and the activation of relevant international agreements to effectively combat this cross-border phenomenon.

1: Email:

taif.ali@utq.edu.iq

2: Email:

DOI

<https://doi.org/10.37651/aujlp.2025.165241.1600>

Submitted: 2/9/2025

Accepted: 24/9/2025

Published: 1/06/2026

Keywords:

Responsibility
Criminal
Crimes
Encryption
Digital Currencies
Comparative Law
Virtual World.

©Authors, 2026, College of Law
University of Anbar. This is an open-
access article under the CC BY 4.0
license (<http://creativecommons.org/licenses/by/4.0/>).



المسؤولية الجنائية عن جرائم التشفير والعملات الرقمية في القانون المقارن م.م طيف علي غالب جلال^١ جامعة ذي قار / كلية القانون

الملخص:

يتناول البحث موضوع الجرائم المرتبطة بالتشفير والعملات الرقمية من منظور قانوني وجنائي، حيث يسلط الضوء على طبيعة هذه الجرائم وتنوعها، مثل الاحتيال المالي، غسل الأموال، والتهرب الضريبي، والتي أصبحت أكثر تعقيداً مع تطور التكنولوجيا الرقمية. كما يناقش التحديات القانونية التي تواجه الجهات التشريعية والقضائية في التصدي لهذه الجرائم، خاصة في ظل غياب إطار قانوني موحد على المستوى الدولي وصعوبة تتبع المعاملات الرقمية.

يركز البحث أيضاً على كيفية تعامل التشريعات الجنائية الوطنية مع هذه الجرائم، ويستعرض مدى كفاية النصوص القانونية الحالية في ردع مرتكبيها، بالإضافة إلى أهمية تطوير قوانين جديدة تتماشى مع طبيعة الجرائم الرقمية. كما يبرز دور التعاون الدولي في تعزيز المسؤولية الجنائية، من خلال تبادل المعلومات، وتوحيد الجهود بين الدول، وتفعيل الاتفاقيات الدولية ذات الصلة، بهدف تحقيق فعالية أكبر في مكافحة هذه الظاهرة العابرة للحدود.

الكلمات المفتاحية:

المسؤولية، الجنائية، جرائم، التشفير، العملات الرقمية، القانون المقارن، العالم الافتراضي.

المقدمة

أولاً- فكرة الموضوع:

تشهد الأنظمة المالية العالمية تحولاً جوهرياً مع صعود العملات الرقمية المشفرة التي أحدثت ثورة في مفهوم القيمة والتبادل المالي، لكن هذه التقنية أحاطت نفسها بهالة من الغموض القانوني والتنظيمي. فبينما تقدم هذه التقنيات فرصاً لتمويل شامل وابتكار مالي غير مسبوق، فإنها أيضاً فتحت الباب على مصراعيه لشكل جديد من الجرائم المالية الذكية التي تتحدى الأنظمة القانونية التقليدية. لقد أصبحت جرائم العملات المشفرة تهديداً دولياً يتطلب استجابة قانونية منسقة وعابرة للحدود.

ثانياً- أهمية الدراسة:

تكتسب هذه الدراسة أهميتها من الطبيعة الاستثنائية للتحديات التي تفرضها جرائم العملات الرقمية على المنظومات القانونية والقضائية. فمن ناحية، تساعد في كشف الثغرات التشريعية في مواجهة هذه الجرائم المستحدثة، ومن ناحية أخرى تقدم تحليلاً مقارناً للاستجابات التشريعية المختلفة حول العالم.

ثالثاً- أسباب اختيار البحث:

تم اختيار هذا الموضوع نظراً لتزايد استخدام العملات الرقمية والتشفير في المعاملات الحديثة، وما يترتب عليه من ظهور أنماط جديدة من الجرائم التي يصعب ضبطها بالوسائل التقليدية. كما أن غياب تشريعات واضحة ومحدثة في العديد من الدول، والحاجة إلى تعاون دولي فعال، يجعل دراسة المسؤولية الجنائية في هذا المجال أمراً ملحاً ومهماً.

رابعاً- مشكلة الدراسة:

تتمحور إشكالية هذه الدراسة حول مدى قدرة التشريعات الجنائية الوطنية والدولية على مواجهة الجرائم الناشئة عن استخدام التشفير والعملات الرقمية، في ظل التطور السريع للتكنولوجيا الرقمية وتعدد صور هذه الجرائم.

السؤال الرئيسي :

إلى أي مدى تُسهم التشريعات الجنائية والتعاون الدولي في تحقيق المسؤولية الجنائية عن الجرائم المرتبطة بالتشفير والعملات الرقمية؟

الأسئلة الفرعية :

١. ما هي طبيعة الجرائم المرتبطة بالتشفير والعملات الرقمية وما أبرز صورها؟
٢. ما التحديات القانونية التي تواجه الجهات المختصة في التصدي لهذه الجرائم؟
٣. كيف تعاملت التشريعات الجنائية الوطنية مع هذه الجرائم؟ وهل تكفي النصوص الحالية لمواجهتها؟
٤. ما دور التعاون الدولي في تعزيز فعالية الملاحقة الجنائية لهذه الجرائم؟
٥. ما مدى الحاجة إلى تطوير إطار قانوني موحد لمواجهة الجرائم الرقمية العابرة للحدود؟

خامساً- نطاق الدراسة:

يرتكز نطاق الدراسة على تحليل المسؤولية الجنائية المترتبة على الجرائم المرتبطة بالتشفير والعملات الرقمية، من خلال استعراض الإطار القانوني الوطني والدولي، وتحديد أوجه القصور في التشريعات، مع التركيز على التحديات القانونية والتقنية، ودور التعاون الدولي في مواجهتها.

سادساً- منهجية الدراسة:

تعتمد هذه الدراسة على المنهج التحليلي المقارن من خلال تحليل النصوص القانونية والتشريعات المختلفة في العديد من الدول، مع التركيز على النماذج الأوروبية والأمريكية

والعربية. كما تستخدم الدراسة المنهج الوصفي في توصيف أنواع جرائم العملات الرقمية وخصائصها.

سابعاً- هدف الدراسة:

تهدف هذه الدراسة إلى بيان الأساس القانوني للمسؤولية الجنائية الناشئة عن جرائم التشفير والعملات الرقمية، وتحليل مدى كفاية التشريعات الجنائية في مواجهتها، مع التركيز على التحديات القانونية والتقنية، واقتراح سبل لتعزيز التعاون الدولي لضمان فعالية الملاحقة الجنائية لهذه الجرائم الحديثة.

ثامناً- هيكلية البحث:

لمعالجة موضوع البحث سنقوم بتقسيمه الى مبحثين سنتناول في المبحث الأول الإطار المفاهيمي والتحديات القانونية لجرائم التشفير والعملات الرقمية، ومن ثم سنتقل للحديث عن آليات المساءلة الجنائية في القانون المقارن في المبحث الثاني.

I. المبحث الأول

الإطار المفاهيمي لجرائم التشفير والعملات الرقمية وتحدياته القانونية

شهد العقد الأخير طفرة هائلة في التطور التكنولوجي، أفرزت العديد من المفاهيم والابتكارات التي غيرت النظم الاقتصادية والمالية التقليدية. وتأتي العملات الرقمية المشفرة، وعلى رأسها البيتكوين، في صدارة هذه الابتكارات، حيث مثلت نقلة نوعية في مفهوم النقود والتحويلات المالية، مؤسسةً لنظام لامركزي يقوم على تقنية سلسلة الكتل التي توفر درجة عالية من الشفافية والأمان^(١)، وعليه، يأتي هذا المبحث لتسليط الضوء على هذه الإشكالية المحورية، من خلال تقسيمه إلى مطلبين أساسيين: حيث نتناول في المطلب الأول مفهوم جرائم التشفير والعملات الرقمية وأنواعها، أما في المطلب الثاني نتناول: التحديات القانونية في مواجهة جرائم التشفير والعملات الرقمية.

I.أ. المطلب الأول

مفهوم جرائم التشفير والعملات الرقمية وأنواعها

شكّلت الثورة الرقمية بيئة خصبة لظهور أنماط مستحدثة من الجرائم، تستغل الطبيعة الفريدة لتقنيات التشفير والعملات الرقمية، يُعدُّ فهم هذه الجرائم من حيث المفهوم والأنواع

(١) أحمد إبراهيم دهبان، "العملات الافتراضية إشكالياتها وأثارها على الاقتصاد المحلي والعالمي"، المؤتمر الدولي الخامس عشر لكلية الشريعة والدراسات الإسلامية، كلية الشريعة جامعة الشارقة، (٢٠١٩): ص ١٢.

الخطوة الأولى نحو تطوير آليات فعالة لمواجهتها، وسنعالج هذا المطلب من خلال التقسيم الآتي:

I.١. الفرع الأول

تعريف جرائم التشفير والعملات الرقمية

تشكل جرائم التشفير والعملات الرقمية نمطاً مستحدثاً من الأنشطة الإجرامية التي تستغل الخصائص الفريدة للتقنيات المالية الحديثة^(١). يمكن تعريف هذه الجرائم على أنها: أنشطة غير مشروعة تستغل تقنيات التشفير والعملات الرقمية كأداة أو كهدف للجريمة، حيث تمثل هذه الجرائم تحولاً جوهرياً في طبيعة الجريمة المنظمة والجرائم المالية التقليدية. تتميز هذه الجرائم بطابعها العابر للحدود والتقني العالي، مما يجعلها تشكل تحدياً غير مسبوق لأجهزة إنفاذ القانون.

أما العنصر التقني لهذه الجرائم يتمثل في استغلال تقنيات التشفير المتقدمة، التي صممت أساساً لتأمين البيانات وحماية الخصوصية، لكنها أصبحت وسيلة للمجرمين لإخفاء هوياتهم وتشفير اتصالاتهم وأنشطتهم غير المشروعة، فالتشفير هنا يعمل كحاجز تقني يحول دون اكتشاف وتحقيق هذه الأنشطة^(٢).

ويتجلى العنصر المالي في استخدام العملات الرقمية المشفرة، التي تعتمد على تقنية البلوك تشين لامركزية، مما يمكن المجرمين من إجراء معاملات مالية سريعة وعابرة للحدود دون الحاجة إلى وسطاء تقليديين مثل البنوك. هذه الخاصية جعلت من العملات المشفرة وسيلة مثالية لتمويل الأنشطة غير المشروعة وتحويل الأموال بسرية.

نلاحظ أنّ هذا التعقيد يجعل من جرائم التشفير والعملات الرقمية ظاهرة إجرامية مركبة، تجمع بين الجرائم المالية التقليدية والجرائم الإلكترونية المتطورة، مما يستدعي تطوير أطر قانونية وقضائية متخصصة للتعامل مع هذا النوع المستجد من التهديدات الأمنية^(٣). بناءً على ما تقدم أستطيع أن أعرف المسؤولية الجنائية الناشئة عن جرائم التشفير والعملات الرقمية بأنها: الالتزام القانوني الذي يتحمله الفرد أو الكيان نتيجة ارتكاب أفعال مجرّمة ترتبط باستخدام تقنيات التشفير أو التعامل بالعملات الرقمية، والتي تؤدي إلى الإضرار بالمصلحة العامة أو الخاصة، وتستوجب مساءلة جنائية وفقاً لأحكام القانون الوطني والدولي، مع الأخذ بعين الاعتبار الطبيعة التقنية المعقدة لهذه الجرائم، وصعوبة ضبطها

(١) أشرف توفيق شمس الدين، "مخاطر العملات الافتراضية في نظر السياسة الجنائية"، مجلة مصر المعاصرة، الجمعية المصرية للاقتصاد السياسي والإحصاء والتشريع، مج ١١٠، ع ٥٣٥، (٢٠١٩): ص ٢٣٧.

(٢) أحمد صبحي العطار، جرائم الاعتداء على المصلحة العامة، القسم الخاص من قانون العقوبات المصري، (مصر: الهيئة المصرية العامة للكتاب، ٢٠٠٤)، ص ١١٦.

(٣) طارق محمد حمزة، النقود الإلكترونية كأحد وسائل الدفع، (بيروت: منشورات زين الحقوقية، ٢٠٠١)، ص ٦٧.

بالوسائل التقليدية، مما يفرض ضرورة تطوير أدوات قانونية وتشريعية تتناسب مع هذا النمط المستحدث من الجريمة.

I.٢.١. الفرع الثاني

أنواع جرائم العملات الرقمية

سننظر لدراسة أهم جرائم العملات الرقمية مع بيان أمثلة واقعية وطرق الوقاية منها وذلك وفق التقسيم الآتي:

أولاً- غسل الأموال عبر العملات الرقمية وأمنيتها الواقعية:

هي عملية إخفاء المصدر غير القانوني للأموال (مثل أموال المخدرات، الرشاوى، التمويل الإرهابي) وتحويلها إلى أموال ذات مظهر قانوني باستخدام شبكات وعمليات رقمية. تعتبر العملات المشفرة بيئة خصبة لغاسلي الأموال بسبب طبيعتها اللامركزية وقدرتها على إجراء معاملات شبه مجهولة^(١).

آلية التنفيذ (كيف تتم): تتبع عملية غسل الأموال عادة ثلاث مراحل رئيسية حتى في العالم الرقمي:

١- الإيداع: إدخال الأموال غير القانونية إلى النظام المالي للعملات المشفرة. يتم ذلك عادة عن طريق:

- شراء عملات رقمية من منصات تداول غير خاضعة للرقابة، أو باستخدام وثائق مزورة.
- استخدام ماكينات الصراف الآلي للعملات المشفرة التي تسمح بإيداع نقدي بحدود معينة دون هوية.

- تحويل الأموال القذرة إلى عملات مستقرة لتثبيت قيمتها.

٢- التغطية: عملية فصل الأموال عن مصدرها غير القانوني عبر سلسلة معقدة من المعاملات لإرباك السلطات.

٣- أمثلة واقعية:

أ- منصة BTC-e كانت واحدة من أكبر منصات غسل الأموال، حيث تمت معالجة مليارات الدولارات من أموال القرصنة والفساد قبل إغلاقها من قبل السلطات.

ب- خدمة Helix: وهي خدمة خلاط للبيتكوين، حيث أدين مؤسسها بتهم غسل أكثر من ٣٠٠ مليون دولار لصالح سوق "داك ويب" الشهير^(٢).

ج- طرق الوقاية والمواجهة في جرائم العملات الرقمية : يتم من خلال التنظيم الحكومي، وذلك بزيادة الضغط على المنصات وخدمات الخلط لتطبيق القوانين.

(١) طارق محمد حمزة، النقود الإلكترونية كأحد وسائل الدفع، مصدر سابق، ص ٨٩.
(٢) أحمد صبحي العطار، جرائم الاعتداء على المصلحة العامة، مصدر سابق، ص ١٢٦.

ثانياً- الاختراق والسرقة الإلكترونية وأمثلتها الواقعية وطرق الوقاية منها:

هي الجرائم التي تنطوي على الاستيلاء غير القانوني على العملات الرقمية من خلال استغلال الثغرات الأمنية في المنصات، التطبيقات، أو أجهزة المستخدمين أنفسهم. وسندرس كل من الاختراق والسرقة الإلكترونية وأمثلتها الواقعية وطرق الوقاية منها وفق التقسيم الآتي:

١- الاختراق:

آلية التنفيذ (كيف تتم): هناك عدة طرق للاختراق والسرقة^(١):

أ- اختراق المنصات المركزية: استهداف البورصات الكبيرة حيث يخزن الملايين من المستخدمين أموالهم. يتم ذلك عبر استغلال ثغرات في كود الموقع، وهجمات التصيد على موظفي المنصة للحصول على مفاتيح الوصول.

ب- اختراق العقود الذكية: استغلال عيب برمجي في عقد ذكي على منصة مثل Ethereum لسحب الأموال التي يفترض أن تكون مؤمنة، وهذا شائع في تطبيقات التمويل اللامركزي .

ج- برامج الفدية : حيث يتم تشفير ملفات ضحية وطلب فدية بعملة رقمية غالباً لفك التشفير.

د- سرقة المحافظ الفردية: عن طريق برامج التصيد: إنشاء مواقع ومنصات مزورة تشبه الأصلية لخداع المستخدمين لإدخال "العبرة الأساسية " أو كلمات المرور.

٢- أمثلة واقعية:

اختراق : (2014) كانت أكبر بورصة للبيتكوين في العالم، حيث سرق منها ٨٥٠,٠٠٠ بيتكوين (قيمتها اليوم عشرات المليارات).^(٢)

٣- طرق الوقاية والمواجهة:^(٣)

أ- التزام المنصات بأعلى معايير الأمن: استخدام التخزين البارد للأموال، والتأكد من تدقيق العقود الذكية من قبل شركات متخصصة.

ب- عدم مشاركة العبرة الأساسية أبداً: مع أي شخص أو على أي موقع إلكتروني.

ثالثاً- الاحتيال عبر العروض الأولية للعملات وآلية تنفيذها وأمثلتها الواقعية وطرق

الوقاية منها:

١-الاحتيال: هي مخططات احتيالية تجمع الأموال من المستثمرين عن طريق الترويج لعملة رقمية أو مشروع وهمي غالباً عبر "العرض الأولي للعملة"، ثم يهرب المطورون بالأموال أو يتلاعبون بسعر العملة لصالحهم^(٤).

(١) شريف غنام، "محفظة النقود الإلكترونية، رؤية مستقبلية"، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، دبي، (٢٠٠٣): ص ١١٧.

(٢) أحمد حسني، "هاكر في الظل.. أكبر سرقة بيتكوين في التاريخ"، مقال منشور على الموقع الإلكتروني: <https://www.youm7.com/story/> تاريخ الزيارة: ٢٠٢٥/٨/٢٦.

(٣) أشرف توفيق شمس الدين، مخاطر العملات الافتراضية في نظر السياسة الجنائية، مصدر سابق، ص ٢٤٦.

(٤) شريف غنام، محفظة النقود الإلكترونية، رؤية مستقبلية، مصدر سابق، ص ١٨١.

٢- آلية التنفيذ (كيف تتم)^(١):

- أ- إنشاء مشروع وهمي : يقوم المحتالون بإنشاء موقع ويب احترافي وورقة بيضاء مليئة بالمصطلحات التقنية والوعود الكبيرة (مثل "سنغير العالم!"، "عائد استثمار هائل!") دون وجود منتج حقيقي أو فريق تقني خلفه.
- ب- الحملة التسويقية استخدام وسائل التواصل الاجتماعي ومنصات الدعاية ودفع للمساعدة في الترويج للمشروع وخلق ضجة (هيبه) حوله لجذب المستثمرين المطموسين.
- ج- جمع الأموال: يطلبون من الناس إرسال أموال إلى عنوان محفظتهم مقابل الحصول على "رموز" أو "عملات" المشروع الجديد.
- د- الهروب: بعد جمع ملايين الدولارات، يختفي الفريق فجأة، ويغلقون الموقع ووسائل التواصل، ويصبح الرمز عديم القيمة تمامًا.
- ٣- أمثلة واقعية:**

(فيتنام): جمعت ٦٦٠ مليون دولار من آلاف المستثمرين قبل أن يختفي المطورون.

٤- طرق الوقاية والمواجهة:

- أ- البحث عن مراجعات المجتمع وردود الفعل من خبراء مستقلين.
- ب- التشكك في وعود العوائد المرتفعة بشكل غير طبيعي: إذا بدا الأمر جيدًا لدرجة يصعب تصديقها، فغالبًا هو احتيال.
- ج- التعامل مع المشاريع ذات الشفافية العالية والتي تخضع لتدقيق من جهات خارجية.

I. ب. المطلب الثاني**التحديات القانونية في مواجهة جرائم التشفير والعملات الرقمية**

تمثل مواجهة جرائم العملات الرقمية تحديًا قانونيًا هائلًا أمام الحكومات والجهات التنظيمية حول العالم. تنبع صعوبة هذه المواجهة من طبيعة هذه التقنية نفسها؛ حيث تتصادم البنية اللامركزية والعبارة للحدود للعملات المشفرة مع القوانين التقليدية التي بُنيت على أساس مركزي وإقليمي، وتواجه الأنظمة القانونية تحديات جذرية في مجالات الاختصاص القضائي، وتتبع الأدلة، وجمعها، والتعاون الدولي، مما يجعل من الصعب جدًا ملاحقة المجرمين واسترداد الأموال المسروقة^(٢)، ويترك الكثير من الضحايا دون حماية أو إنصاف، بناءً على ما سبق، سندرس هذا المطلب وفق التقسيم الآتي:

(١) سمير رضوان، المشتقات المالية ودورها في إدارة المخاطر ودور الهندسة المالية في صناعة أدواتها ، دراسة مقارنة بين النظم الوضعية وأحكام الشريعة الإسلامية ، الطبعة الأولى، (مصر: دار النشر للجامعات ، ٢٠٠٩)، ص ١٥٩.

(٢) أحمد إبراهيم دهشان العملات الافتراضية إشكالياتها وأثارها على الاقتصاد المحلي والعالمي، مصدر سابق، ص ٢٩.

I. ب. ١. الفرع الأول

التحديات التقنية والقانونية

تمثل الخصائص الفريدة للعملات الرقمية، مثل اللامركزية واستخدام التشفير المتقدم، تحديات جذرية أمام الأطر التقليدية للرقابة والقانون. هذه التحديات تعيق جهود السلطات في تتبع الأنشطة غير المشروعة وحماية المستخدمين، مما يتطلب تطوير أدوات وتشريعات جديدة لمواكبة هذه التكنولوجيا المتطورة.

أولاً- اللامركزية وغياب السلطة الرقابية

اللامركزية هي العمود الفقري للعديد من العملات الرقمية مثل البيتكوين والإيثريوم، وهي تعني أن النظام لا يخضع لسيطرة أي سلطة مركزية مثل البنوك أو الحكومات. بدلاً من ذلك، يتم توزيع السيطرة والتحقق من المعاملات عبر شبكة واسعة من أجهزة الكمبيوتر حول العالم.^(١)

١- آثار اللامركزية على الرقابة والقانون:

أ- عدم وجود وسيط مركزي: في النظام المالي التقليدي، تتحكم البنوك والمؤسسات المالية في عمليات تداول الأموال وتعمل كوسطاء يمكن الرجوع إليهم في حالة النزاعات أو الأنشطة المشبوهة. في المقابل، تتيح العملات الرقمية تحويل الأموال مباشرة بين الأفراد دون الحاجة إلى وسيط مالي. هذا يلغي نقطة الرقابة التقليدية ويجعل من الصعب مراقبة المعاملات.

ب- صعوبة تتبع التحويلات المالية: طبيعة العملات الرقمية اللامركزية وصعوبة تتبع التحويلات المالية تجعل من الصعب مراقبتها. وهذا يمثل تحديًا كبيرًا لمكافحة غسل الأموال وتمويل الإرهاب.

ج- التحدي القانوني للاختصاص القضائي: المعاملات عبر الحدود ولا تتبع سلطة مركزية، يصعب تحديد الجهة القانونية المسؤولة عن التحقيق في الجرائم. فالمجرم يمكنه operates من دولة ذات قوانين متساهلة، بينما يقع الضحايا في دول أخرى^(٢).

٢- محاولات التغلب على هذا التحدي:

أ- تطوير أطر تنظيمية مرنة: بعض الدول، مثل الإمارات العربية المتحدة، بدأت في إنشاء أطر ترخيص للشركات التي تعمل في مجال العملات الرقمية، مما يضمن وجود درجة من الرقابة والامتثال للقوانين المحلية.

(١) راشد عبد الرحمن أحمد محمد، "العملات الافتراضية ووسائل الدفع الإلكترونية البنوكوين نموذجاً"، مجلة العلوم الشرعية جامعة القصيم، مج ١٤ ع ٣، (٢٠٢١): ص ٣١١.

(٢) أحمد إبراهيم دهشان العملات الافتراضية إشكالياتها وأثارها على الاقتصاد المحلي والعالمي، مصدر سابق، ص ٤٧.

- ب- تعزيز التعاون الدولي: أصبح من الضروري تعزيز التعاون بين الدول لوضع معايير عالمية لمراقبة وتحليل المعاملات عبر السلاسل المختلفة.
- ج- اعتماد تقنيات المراقبة المتقدمة: تستخدم السلطات والشركات أدوات متقدمة لمراقبة سلسلة الكتل وتحليل البيانات للكشف عن الأنماط المشبوهة، مثل الخدمات التي تقدمها شركات مثل FOCAL التي تستخدم الذكاء الاصطناعي.

ثانياً- التشفير المتقدم

يعد التشفير حجر الزاوية في أمان العملات الرقمية، حيث يضمن سرية وسلامة المعاملات ويحمي هويات المستخدمين. ومع ذلك، فإن هذه الميزة نفسها تشكل تحدياً كبيراً إنفاذ القانون.^(١)

١- آثار التشفير المتقدم على الرقابة والقانون:

- أ- إخفاء هويات الأطراف: على الرغم من أن معاملات البلوكتشين تكون علنية وشفافة (يمكن رؤية عناوين المحافظ والمبالغ)، إلا أن هويات أصحاب هذه العناوين تظل مجهولة في كثير من الأحيان. يتم استخدام عناوين محفظة مشفرة بدلاً من المعلومات الشخصية، مما يجعل ربط المعاملة بهوية حقيقية أمراً صعباً دون تقنيات متخصصة.^(٢)
- ب- صعوبة كسر التشفير: التشفير المتقدم (مثل خوارزميات التجزئة والتوقيعات الرقمية) يجعل من المستحيل عملياً اختراق المعاملات أو تعديلها بمجرد تأكيدها على الشبكة. هذه القوة الحسابية تحمي النظام ولكنها أيضاً تحمي المجرمين الذين يستغلونها.
- ٢- محاولات التغلب على هذا التحدي^(٣):

- أ- تحليل البيانات: تطورت صناعة كاملة حول تحليل سلسلة الكتل، حيث تستخدم شركات مثل Chainalysis و Elliptic أدوات متطورة لربط عناوين المحافظ بالهويات الحقيقية من خلال تتبع أنماط التدفق والبحث عن ثغرات في إجراءات إخفاء الهوية التي يستخدمها المجرمون.^(٤)
- ب- تعزيز متطلبات معرفة العميل (KYC): تفرض العديد من المنصات المركزية الآن إجراءات صارمة للتحقق من هوية العملاء (KYC) قبل السماح لهم بالتداول أو السحب. هذا يخلق نقطة حيث يمكن ربط الهوية الحقيقية بعنوان المحفظة.

(١) سمير رضوان، المشتقات المالية ودورها في إدارة المخاطر ودور الهندسة المالية في صناعة أدواتها ، مصدر سابق، ص ١٦٣.

(٢) راشد عبد الرحمن أحمد محمد، العملات الافتراضية ووسائل الدفع الإلكترونية البتكوين نموذجاً، مصدر سابق، ص ٣٥٢.

(٣) المصدر ذاته، ص ٣٦١.

(٤) سبتي بن مصيلب سبتي، "العملات الافتراضية دراسة فقهية تأصيلية"، مجلة جامعة الملك عبد العزيز، مج ٢٨، ع ١٢، (٢٠٢٠): ص ٤١٦.

I. ب. ٢. الفرع الثاني

التحديات المتعلقة بالاختصاص القضائي:

تمثل قضية الاختصاص القضائي أحد أكبر العقبات العملية والقانونية في ملاحقة جرائم العملات الرقمية. حيث تتعارض الطبيعة الافتراضية والعالمية لهذه الأصول مع النظام القانوني التقليدي القائم على الحدود الجغرافية والسيادة الوطنية، مما يخلق متاهة قانونية يصعب على السلطات التنقل فيها^(١).

أولاً- الطبيعة العابرة للحدود :

الإنترنت لا يعرف حدوداً، والعملات الرقمية هي نتاج هذا الفضاء الافتراضي العالمي. معاملة واحدة من محفظة رقمية يمكن أن تبدأ في دولة، وتُعالج عبر خوادم في قارة ثانية، ويستلمها مستخدم في قارة ثالثة، كل ذلك في غضون دقائق.

١- آثار الطبيعة العابرة للحدود:

صعوبة تحديد موقع الجريمة: مكان ارتكاب الفعل: أين تم ارتكاب الجريمة بالضبط؟ هل هو مكان وجود المجرم؟ أم مكان وجود الخوادم التي تستضيف المنصة المخترقة؟ أم مكان عقدة التعدين التي المعاملة؟ أم موقع الضحية؟

مكان وقوع الأثر: الأضرار المالية للضحية قد تقع في دولة مختلفة عن دولة المجرم. تسمح القوانين في بعض الدول بمقاضاة المجرمين إذا وقع الضرر على أحد مواطنيها، حتى لو كان المجرم خارج البلاد، ولكن تطبيق هذا على العملات الرقمية معقد.

تعقيد عملية جمع الأدلة والتفتيش: تتطلب جمع الأدلة الرقمية الحاسمة مثل سجلات الخوادم، عناوين، محتويات المحافظ (التعاون مع سلطات دول أخرى. عملية "المساعدة القانونية المتبادلة" بطيئة جداً وقد تستغرق شهوراً أو سنوات، بينما يمكن للمجرمين تحويل أو صرف الأموال المسروقة في دقائق^(٢).

تحديات تنفيذ الأحكام ومصادرة الأصول: حتى إذا تمت إدانة مجرم في دولة ما، كيف يمكن مصادرة العملات المسروقة إذا كانت محفوظة في محفظة رقمية ومشتتة عبر عدة سلاسل كتل؟

إذا تم تتبع الأموال إلى منصة تداول في دولة أخرى، فإن تنفيذ أمر قضائي بمصادرتها يتطلب اعترافاً قضائياً من تلك الدولة، والذي قد لا يكون ممكناً أو قد يستغرق وقتاً طويلاً.

٢- اختلاف التشريعات بين الدول

لا يوجد إجماع عالمي على كيفية تعريف أو معاملة أو تنظيم العملات الرقمية. هذا الاختلاف يخلق "ملاذات أمنة" للمجرمين ومناطق رمادية قانونية.

(١) أحمد قاسم فرج، "العملات الافتراضية في دولة الإمارات العربية المتحدة - الحاجة إلى إطار قانوني لمواجهة مخاطرها، دراسة مقارنة"، بحث منشور في مجلة جامعة الشارقة، العدد ٢، (٢٠٠٩): ص ٧١٣.

(٢) سبتي بن مصيليت سبتي، العملات الافتراضية دراسة فقهية تأصيلية، مصدر سابق، ص ٤٢٦.

آثار اختلاف التشريعات:

أ- تعارض القوانين : ما يعتبر نشاطاً مشروعاً في دولة قد يكون جريمة في دولة أخرى. على سبيل المثال، تختلف المواقف القانونية تجاه العملات الرقمية بشكل كبير حول العالم، هذا الاختلاف يمكن أن يؤدي إلى رفض دولة تسليم مجرم لأن الفعل الذي ارتكبه لا يعتبر جريمة في أراضيها.^(١)

ب- عدم وجود تعريف قانوني موحد: هل العملة الرقمية هي سلعة؟ أم أصل مالي؟ أم عملة؟ أم غير ملموس؟ هذا الاختلاف في التصنيف يؤثر بشكل مباشر على الجهة المنظمة (هيئة الأسواق المالية أم البنك المركزي أم غيرها)، والقوانين التي ستطبق عليها، وكيفية التعامل معها في القضايا الضريبية والجنائية^(٢).

مما تقدم نجد: تخلق التحديات المتعلقة بالاختصاص القضائي - الناتجة عن الطبيعة العابرة للحدود واختلاف التشريعات الوطنية - بيئة مثالية للمجرمين للعب على الاختلافات والثغرات بين الأنظمة القضائية. مواجهة هذا التحدي تتطلب حلاً جذرياً يعتمد على التعاون الدولي بشكل غير مسبوق، يتجاوز البطء البيروقراطي الحالي.

II. المبحث الثاني**أحكام المسؤولية الجنائية لجرائم التشفير والعملات الرقمية**

تمثل الجرائم المرتبطة بالعملات الرقمية تحدياً عصبياً أمام المنظومات القانونية في مختلف الدول، بالنظر إلى الطبيعة العابرة للحدود واللامركزية لهذه الأصول المالية، والتي تستغل الثغرات في الأنظمة التقليدية. وقد سارعت العديد من التشريعات إلى تطوير آليات مساءلة جنائية متخصصة لمواكبة هذه الجرائم المستحدثة، تتراوح بين التكيف مع النصوص القائمة وإنشاء أطر قانونية جديدة بالكامل^(٣)، بناءً على ما سبق، سندرس هذا المبحث في مطلبين، حيث نتناول في المطلب الأول: النماذج التشريعية لمواجهة جرائم العملات الرقمية، أما في المطلب الثاني نتناول: دور التعاون الدولي في تعزيز المسؤولية الجنائية.

(١) أحمد قاسم فرج، العملات الافتراضية في دولة الإمارات العربية المتحدة - الحاجة إلى إطار قانوني لمواجهة مخاطرها، مصدر سابق، ص ٧١٤.

(٢) المصدر ذاته، ص ٧١٥.

(٣) سمير رضوان، المشتقات المالية ودورها في إدارة المخاطر ودور الهندسة المالية في صناعة أدواتها ، دراسة مقارنة بين النظم الوضعية وأحكام الشريعة الإسلامية ، مصدر سابق، ص ٢٤٢.

II. أ. المطلب الأول

موقف التشريعات الجنائية لمواجهة جرائم التشفير العملات الرقمية

تمثل جرائم العملات الرقمية تحديًا معقدًا للمشرعين حول العالم بسبب طبيعتها العابرة للحدود والتقنيات المتطورة المستخدمة فيها. وقد تباينت الاستجابات التشريعية لها بين المناطق المختلفة، وسنركز هنا على النموذجين الأوروبي والأمريكي كأحد أكثر النماذج تطورًا وتأثيرًا، وعليه سندرس هذا المطلب وفق التقسيم الآتي:

II. أ. ١. الفرع الأول

النموذج الأوروبي والأمريكي:

يتميز النموذج الأوروبي والأمريكي بتبني استراتيجيات متطورة وشمولية لمواجهة جرائم العملات الرقمية، مع وجود بعض الاختلافات في النهج والأدوات التشريعية بينهما. أولاً- النموذج الأوروبي

يعتمد الاتحاد الأوروبي على إطار تنظيمي موحد يركز على تعزيز الشفافية وحماية المستهلكين ومكافحة الأنشطة غير المشروعة:^(١)

١. التشريعات الموحدة: أصدر الاتحاد الأوروبي "لوائح نقل الأموال والمعلومات المصاحبة لتحويلات بعض العملات المشفرة" والتي تهدف إلى تعقب تحويلات الأصول الافتراضية لمكافحة غسل الأموال وتمويل الإرهاب. هذه اللوائح تلزم مقدمي خدمات الأصول الافتراضية (VASPs) بجمع ومشاركة معلومات حول مرسلي ومستلمي التحويلات.

٢. التعاون عبر الحدود: يُعد اليوروبول (Europol) أحد الأعمدة الرئيسية في هذا النموذج، حيث يدير المركز الأوروبي لمكافحة الجريمة الإلكترونية (EC3) الذي يعزز التعاون بين دول الاتحاد الأوروبي في تحقيقات الجرائم الإلكترونية، بما في ذلك جرائم العملات المشفرة. كما يعقد مؤتمرات دورية مع الإنترنتبول لتبادل الخبرات والابتكارات في مكافحة الجريمة الإلكترونية.

٣. مصادرة الأصول: تتعاون الدول الأوروبية في العمليات الدولية لمصادرة الأصول غير المشروعة، كما حدث في "عملية First Light" التي شاركت فيها ٦١ دولة وتم خلالها مصادرة ٢٥٧ مليون دولار أمريكي وتجميد آلاف الحسابات المصرفية المرتبطة بالاحتيال عبر الإنترنت، بما في ذلك العملات المشفرة.^(٢)

(1)Godlove 'Regulatory Overview of virtual currency, oklahoma Journal of law and technology 'Jan.2014, vol,10, Num. 1

(٢) أحمد سعد على، "العملات الافتراضية المشفرة ماهيتها خصائصها تكيفاتها الفقهية بيتكوين نموذجاً"، مجلة دار الإفتاء المصرية، ع ٣٩، (٢٠١٩): ص ١٣٣.

ثانياً- النموذج الأمريكي

تبنى الولايات المتحدة الأمريكية نهجاً متعدد الأوجه يجمع بين الإنفاذ الصارم للقانون والتكيف مع التحديات التقنية والفريدة التي تطرحها العملات الرقمية^(١):

١. الإنفاذ الجنائي المتخصص: أنشأت الولايات المتحدة وحدات متخصصة مثل "فرقة الاستغلال الرقمي للأصول" التابعة لمكتب التحقيقات الفيدرالي (FBI)، والتي تركز على تحليل البلوك تشين ومصادرة الأصول الرقمية. كما يلعب جهاز الخدمة السرية دوراً رئيسياً في حماية النظام المالي من الاستخدام غير المشروع للأصول الرقمية منذ عام ١٨٦٥، حيث يتعامل مع جرائم مثل الاحتيال ببطاقات الائتمان وبرمجيات الفدية.

٢. التوجيهات السياسية الحديثة: في أبريل ٢٠٢٥، أصدرت وزارة العدل الأمريكية مذكرة جديدة بإنهاء ما يُعرف بـ "التنظيم من خلال الملاحقة القضائية". تركز هذه السياسة على ملاحقة الأفراد الذين يستخدمون العملات الرقمية لارتكاب جرائم مثل الاحتيال على المستثمرين، أو تمويل الإرهاب، أو الاتجار بالمخدرات، أو الجرائم المنظمة، بدلاً من ملاحقة الانتهاكات التنظيمية فقط ما لم تكن هناك أدلة على علم المتهم بالمخالفة وإرادتها. كما تم حل "فريق إنفاذ العملات المشفرة الوطني" وإعادة توزيع موارده.

٣. التركيز على حماية الضحايا: تهدف السياسة الأمريكية الجديدة أيضاً إلى تعويض ضحايا جرائم العملات الرقمية من خلال عملية المصادرة والرد، حيث يُعاد إلى الضحايا قيمة أصولهم الرقمية في وقت ارتكاب الجريمة. كما تبحث وزارة العدل عن تغييرات تشريعية لتعويض الضحايا عن الزيادة في قيمة الأصول الرقمية بعد الجريمة إذا كانوا سيستفيدون منها لولا الاحتيال^(٢).

٤. التعاون مع القطاع الخاص: تتعاون الوكالات الأمريكية مثل الإنترنت واليونودك مع شركات متخصصة في تحليل البلوك تشين مثل لتطوير أدوات الطب الشرعي الرقمي وتدريب أجهزة إنفاذ القانون على تتبع المعاملات غير المشروعة.

II. أ. ٢. الفرع الثاني

النموذج العربي والإفريقي

يُمثل النموذج العربي والإفريقي حالة دراسة مثيرة للاهتمام في مواجهة جرائم العملات الرقمية، حيث يجسد سلسلة من التحديات المشتركة والاستجابات المتباينة، تتراوح بين التشريعات الصارمة والمقاربات الحذرة. وعلى الرغم من اختلاف السياقات الاقتصادية

(1) DeFiLippi Bitcoin: A Regulatory Nightmare to a Libertarian Dream, Internet Policy Review 2014,3 (2) .

(2) Kien-Meng Ly, coining Bitcoin's, 'Legal-Bits': Examining the regulatory framework for bitcoin and virtual currencies, Harvard Journal of Law, Technology, Vole .27,Num. 2,spring 2014.

والأمنية بين الدول العربية والأفريقية، إلا أن العديد منها يتشارك في مواجهة تهديدات متشابهة مثل الاحتيال المالي وغسل الأموال عبر هذه التقنيات الناشئة^(١).

أولاً- السمات المشتركة والتحديات: تواجه العديد من الدول العربية والأفريقية تحديات متقاطعة في مجال مكافحة جرائم العملات الرقمية أبرزها نقص الأطر القانونية المتخصصة، والقيود التقنية والبشرية في مجال التحقيق والرقابة، إضافة إلى صعوبات في مواكبة السرعة المتزايدة للابتكار المالي. كما أن الطبيعة العابرة للحدود لهذه الجرائم تفرض ضغوطاً إضافية على الأنظمة القضائية والنفاذية التي تعاني أساساً من محدودية في موارد التعاون الدولي. ومع ذلك، بدأت عدة دول في السنوات الأخيرة بتطوير استجابات تشريعية وهيكلية تتناسب مع أولوياتها المحلية^(٢).

ثانياً- الاستجابات التشريعية والهيكلية: اتجهت بعض الدول العربية والأفريقية إلى تبني تشريعات صريحة لتنظيم العملات الرقمية ومواجهة الجرائم المرتبطة بها. على سبيل المثال، أصدرت دولة الإمارات العربية المتحدة تشريعات متقدمة من خلال هيئة الأوراق المالية والسلع، وأنشأت مناطق حرة ذات أطر تنظيمية جاذبة ولكن تحت رقابة صارمة لمكافحة غسل الأموال. كما طورت مصر والمغرب أطراً رقابية تتطلب من مقدمي خدمات الأصول الرقمية التسجيل والامتثال لمتطلبات مكافحة غسل الأموال وتمويل الإرهاب^(٣).

ثالثاً- التعاون الإقليمي وبناء القدرات: تبذل مجموعة من الدول العربية جهوداً ملحوظة في تعزيز التعاون الأمني والقضائي عبر آليات مثل مكتب التنسيق لمكافحة الجريمة الإلكترونية في مجلس التعاون لدول الخليج العربية، أو من خلال تفعيل شبكات التبادل المعلوماتي بين البنوك المركزية. وفي أفريقيا، تشارك منظمات مثل الاتحاد الأفريقي واللجنة الأفريقية لمكافحة غسل الأموال في وضع مبادئ توجيهية وتنظيم ورش عمل لبناء قدرات الكوادر الوطنية في مجال التحقيق في الجرائم المالية الرقمية^(٤).

رابعاً- المعوقات والتوجهات المستقبلية: لا تزال معظم الدول العربية والأفريقية تواجه معوقات كبيرة أبرزها عدم كفاية البنى التحتية التقنية، ونقص الخبراء المختصين في تحليل سلاسل الكتل، إضافة إلى صعوبات في تنسيق الإجراءات عبر الحدود. ومع ذلك، فإن الاتجاه العام يتجه نحو مزيد من التنظيم الواضح، واستحداث وحدات متخصصة في أجهزة الشرطة

(١) أحمد حسن، "الموكلين استخدام الجماعات والمنظمات الإرهابية للتقنيات الافتراضية العملات الافتراضية نموذجاً"، الاتحاد العربي للمكاتب والمعلومات، ع ٣٠، (٢٠٢١): ص ١٤٨.

(٢) السيد محمد السيد عمران، الالتزام بالإعلام الإلكتروني قبل التعاقد عبر شبكة الانترنت، (القاهرة: الدار الجامعي ٢٠٠٦)، ص ٧١.

(٣) رؤوف عبيد، السببية الجنائية بين الفقه والقضاء دراسة تحليلية مقارنة، الطبعة الرابعة، (مصر: دار الفكر العربي، ٢٠٠٧)، ص ١٢٩.

(4) Alcon, legitimizing Bitcoin ; Policy Recommendations 'Nov.2013 <https://groups>

والنيابات للتعامل مع هذه النوعية من الجرائم، والاستفادة من الشراكات الدولية لتعزيز القدرات المحلية.^(١)

بالنتيجة: يتميز النموذج العربي والإفريقي بالتباين والتطور التدريجي، حيث تسعى الدول الأكثر تقدماً تنظيمياً إلى خلق بيئة آمنة لجذب الاستثمار التكنولوجي دون إغفال متطلبات الحماية الأمنية، بينما لا تزال دول أخرى في مرحلة وضع الأسس التشريعية الأولى. على الرغم من التحديات، فإن الوعي المتزايد بمخاطر الجرائم الإلكترونية يدفع نحو مزيد من التعاون وتبني أفضل الممارسات الدولية، مع محاولة تكييفها مع الخصوصيات المحلية.

II. ب. المطلب الثاني

دور التعاون الدولي في تعزيز المسؤولية الجنائية

يُعد التعاون الدولي ركيزة أساسية في تعزيز فعالية المساءلة الجنائية عن جرائم العملات الرقمية، نظراً للطبيعة العابرة للحدود التي تميز هذه الجرائم، والتي تتخطى قدرة أي دولة بمفردها على مواجهتها. وتتنوع آليات هذا التعاون لتشكل شبكة معقدة من الترتيبات القانونية والمؤسسية تهدف إلى تسهيل تبادل المعلومات، وتنفيذ الإجراءات القضائية، ومصادرة العائدات الإجرامية^(٢)، وعليه سندرس هذا المطلب وفق التقسيم الآتي:

II. ب. ١. الفرع الأول

آليات التعاون الدولي

تقوم آليات التعاون الدولي على عدة أسس، أهمها الاتفاقيات الدولية الثنائية والإقليمية، والتي تنشئ أطراً ملزمة للدول الأطراف في مجالات المساعدة القانونية المتبادلة وتسليم المجرمين. كما تلعب المنظمات الدولية دوراً محورياً في تنسيق الجهود ووضع المعايير المشتركة.

على الصعيد العالمي، تمثل اتفاقيات مثل اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية (اتفاقية باليرمو) واتفاقية ميريدا لمكافحة الفساد أطراً قانونية دولية تلتزم الدول من خلالها بتقديم المساعدة في جمع الأدلة وتجميد الأصول وتسليم المشتبه بهم. وتعمل أجهزة مثل الإنتربول واليونسكو على تسهيل التواصل العملي بين أجهزة إنفاذ القانون في

(١) السيد محمد السيد عمران، الالتزام بالإعلام الإلكتروني قبل التعاقد عبر شبكة الانترنت، مصدر سابق، ص ١٢٨.

(٢) جميل عبد الباقي الصغير، "الجرائم الناجمة عن الحاسب الآلي والإنترنت"، المؤتمر الدولي الأول لقانون الإنترنت نحو علاقة قانونية وإدارية واقتصادية وسياسية واجتماعية جديدة - المنظمة العربية للتنمية، (٢٠٠٥): ص ٤٧.

مختلف الدول، حيث ينظم الإنترنت نشر الإنذارات الدولية ويدير قواعد بيانات للمعلومات الحيوية المتعلقة بالمجرمين والتحقيقات الجارية^(١).

على المستوى الإقليمي، تظهر نماذج ناجحة للتعاون مثل اليوروبول في الاتحاد الأوروبي، الذي يوفر منصة للتبادل الفوري للمعلومات الاستخباراتية والعملية بين الدول الأعضاء، ويدعم التحقيقات المشتركة عبر فرق عمل مشتركة. كما تسهم المنظمات الإقليمية العربية والإفريقية، كالمجلس العربي للدفاع الاجتماعي أو اللجنة الأفريقية لمكافحة غسل الأموال، في وضع مبادئ توجيهية موحدة وتعزيز التنسيق بين البنوك المركزية وأجهزة الرقابة المالية^(٢).

أما على المستوى الثنائي، فإن اتفاقيات المساعدة القانونية المتبادلة وتفاهات تسليم المجرمين بين الدول تظل الآلية الأكثر مباشرة وفعالية في كثير من الحالات. هذه الاتفاقيات تسمح للسلطات القضائية بطلب وإجراء إجراءات محددة، مثل استجواب الشهود، وتنفيذ أوامر التفتيش والحجز، وتجميد وتحويل العائدات الإجرامية، بما في ذلك العملات الرقمية^(٣).

بالإضافة إلى ذلك، تبرز أهمية الشراكات بين القطاع العام والخاص كآلية تعاون مبتكرة. حيث تعتمد أجهزة إنفاذ القانون في العديد من الدول على الخبرة التقنية والتحليلات المتقدمة التي تقدمها شركات متخصصة في تحليل سلاسل الكتل لتتبع الحركة غير المشروعة للأصول الرقمية عبر الحدود وتحديد هويات المشتبه بهم.

ختامًا، يمكن القول إن نجاح آليات التعاون الدولي في تعزيز المسؤولية الجنائية عن جرائم العملات الرقمية مرهون بمدى توافق الإرادات السياسية والقانونية بين الدول، وقدرتها على تطوير أطر مرنة وسريعة تستجيب للطبيعة الديناميكية لهذه الجرائم، مع الحفاظ على التوازن بين متطلبات العدالة وحقوق الأفراد.

II. ب. ٢. الفرع الثاني

التوصيات المستقبلية

لتعزيز دور التعاون الدولي في مكافحة جرائم العملات الرقمية وضمان فعالية المساءلة الجنائية، يمكن طرح جملة من التوصيات المستقبلية التي تستهدف معالجة الثغرات الحالية ومواكبة التطورات المتسارعة في هذا المجال^(٤).

(١) أحمد حسن الموكلين استخدام الجماعات والمنظمات الإرهابية للتقنيات الافتراضية العملات الافتراضية نموذجاً، مصدر سابق، ص ١٥١.

(٢) السيد محمد السيد عمران، الالتزام بالإعلام الإلكتروني قبل التعاقد عبر شبكة الانترنت، (القاهرة: الدار الجامعي، ٢٠٠٦)، ص ٨١.

(٣) جميل عبد الباقي الصغير، الجرائم الناجمة عن الحاسب الآلي والإنترنت – المؤتمر الدولي الأول لقانون الإنترنت نحو علاقة قانونية وإدارية واقتصادية وسياسية واجتماعية جديدة، مصدر سابق، ص ٩١.

(٤) أحمد حسن الموكلين استخدام الجماعات والمنظمات الإرهابية للتقنيات الافتراضية العملات الافتراضية نموذجاً، مصدر سابق، ص ١٥٦.

أولاً- ينبغي العمل على تطوير أطر قانونية دولية موحدة تتسم بالمرونة والوضوح، وذلك من خلال تبني اتفاقيات دولية خاصة بجرائم الفضاء الإلكتروني والعملات الرقمية، أو تعديل الاتفاقيات القائمة لتشمل نصوصاً صريحة تغطي هذه الجرائم الناشئة. ويجب أن تركز هذه الأطر على توحيد التعريفات القانونية للجرائم المرتبطة بالعملات الرقمية وتسهيل تبادل الأدلة الرقمية بين الدول.

ثانياً- يتعين تعزيز القدرات الفنية والبشرية لأجهزة إنفاذ القانون والسلطات القضائية في الدول النامية على وجه الخصوص، من خلال برامج تدريبية متخصصة تهدف إلى بناء كفاءات في مجال التحقيق الجنائي الرقمي، وتحليل سلاسل الكتل، وتتبع الأصول المشفرة. ويمكن أن تقدم المنظمات الدولية والدول المتقدمة الدعم اللازم في هذا المجال.

ثالثاً- يجب تشجيع إنشاء شبكات تعاون إقليمية ودولية متخصصة في مكافحة جرائم العملات الرقمية، على غرار شبكات التبادل المعلوماتي بين البنوك المركزية، بحيث تعمل هذه الشبكات على تيسير تدفق المعلومات بشكل آمن وسريع بين الدول الأعضاء، والمساهمة في تنسيق العمليات المشتركة لملاحقة المجرمين عبر الحدود.

رابعاً- من الضروري تطوير آليات مبتكرة للتعاون بين القطاع العام والخاص، حيث يمكن للشركات التقنية المتخصصة ومقدمي خدمات العملات الرقمية أن يلعبوا دوراً محورياً في مساعدة الأجهزة الأمنية من خلال توفير البيانات التقنية والخبرات اللازمة، مع ضمان احترام معايير الخصوصية وحماية البيانات.

خامساً- يجب العمل على معالجة العقوبات القانونية والإجرائية التي تواجه عملية المصادرة والعائدات الإجرامية ذات الطبيعة الرقمية، وتطوير آليات سريعة وفعالة لاسترداد الأصول وتوزيعها على الضحايا عبر الحدود، مع مراعاة المبادئ الأساسية للعدالة^(١).

أخيراً، يتوجب تعزيز دور البحث العلمي والدراسات المستقبلية في هذا المجال، من خلال تشجيع المراكز البحثية والأكاديمية على دراسة الظاهرة وتحليل التحديات الناشئة، مما يسهم في تطوير رؤى استباقية واستراتيجيات فعالة لمواجهة هذه الجرائم.

وفي الختام، فإن تفعيل هذه التوصيات يتطلب إرادة سياسية حقيقية وتعاوناً مستمراً بين جميع الأطراف المعنية على الصعيد الدولي، لضمان تحقيق الأمن والاستقرار في الفضاء الرقمي وحماية المصالح الاقتصادية للدول والأفراد.

(١) أحمد حسن الموكلين استخدام الجماعات والمنظمات الإرهابية للتقنيات الافتراضية العملات الافتراضية نموذجاً، مصدر سابق، ص ١٥٩.

الخاتمة

بعد دراسة متعمقة للإطار المفاهيمي والتحديات القانونية لجرائم التشفير والعملات الرقمية، وتحليل آليات المساءلة الجنائية في القانون المقارن، يمكن القول إن مواجهة هذه الجرائم تمثل تحدياً معقداً يتطلب مقاربة شاملة ومتعددة المستويات. لقد كشفت الدراسة عن فجوة تشريعية كبيرة بين السرعة المتسارعة للتطور التكنولوجي وبطء الاستجابة القانونية، مما يستدعي ضرورة تطوير أطر قانونية مرنة وقادرة على مجاراة هذه التحولات الرقمية. كما أظهرت الدراسة أن فعالية المواجهة لن تتحقق دون تعاون دولي حقيقي يضمن تبادل الخبرات والمعلومات ويتخطى الحدود الجغرافية والسيادية، وقد توصلنا من خلال هذه الدراسة إلى جملة من النتائج والمقترحات:

أولاً- النتائج:

١. تعدد صور الجرائم الرقمية المرتبطة بالتشفير والعملات الرقمية، مثل الاحتيال، غسل الأموال، والتمويل غير المشروع، مما يجعلها تحدياً قانونياً متجدداً.
٢. قصور التشريعات الجنائية التقليدية في مواكبة التطورات التقنية، حيث لا تزال العديد من النصوص القانونية غير قادرة على استيعاب طبيعة هذه الجرائم الحديثة.
٣. صعوبة الإثبات الجنائي في الجرائم الرقمية بسبب الطابع غير المادي للعملات المشفرة، واعتمادها على شبكات لا مركزية يصعب تتبعها.
٤. غياب التنسيق الدولي الفعال في مكافحة هذه الجرائم، مما يتيح للمجرمين استغلال الفجوات القانونية بين الدول.
٥. الحاجة إلى تأصيل المسؤولية الجنائية للأشخاص الطبيعيين والاعتباريين المتورطين في هذه الجرائم، بما في ذلك منصات التداول ومقدمي الخدمات الرقمية.

ثانياً- المقترحات:

١. تحديث التشريعات الجنائية الوطنية لتشمل تعريفاً دقيقاً لجرائم التشفير والعملات الرقمية، وتحديد العقوبات المناسبة لها.
٢. إنشاء وحدات متخصصة داخل الأجهزة القضائية والأمنية لمكافحة الجرائم الرقمية، وتدريب الكوادر على التقنيات الحديثة.
٣. تعزيز التعاون الدولي من خلال الاتفاقيات الثنائية ومتعددة الأطراف، وتبادل المعلومات بين الدول بشأن الجرائم العابرة للحدود.
٤. تبني إطار قانوني موحد عالمياً لتنظيم استخدام العملات الرقمية وضبط الجرائم المرتبطة بها، بما يضمن العدالة الجنائية.
٥. إشراك القطاع الخاص، وخاصة منصات التداول ومطوري البرمجيات، في جهود الوقاية والكشف عن الجرائم الرقمية، ضمن مسؤولية قانونية واضحة.

قائمة المصادر والمراجع

أولاً- الكتب:

١. أحمد صبحي العطار، جرائم الاعتداء علي المصلحة العامة، القسم الخاص من قانون العقوبات المصري، مصر: الهيئة المصرية العامة للكتاب، ٢٠٠٤.
٢. رؤوف عبيد، السببية الجنائية بين الفقه والقضاء دراسة تحليلية مقارنة، الطبعة الرابعة، مصر: دار الفكر العربي، ٢٠٠٧.
٣. سمير رضوان، المشتقات المالية ودورها في إدارة المخاطر ودور الهندسة المالية في صناعة أدواتها ، دراسة مقارنة بين النظم الوضعية وأحكام الشريعة الإسلامية ، الطبعة الأولى، مصر: دار النشر للجامعات ، ٢٠٠٩.
٤. السيد محمد السيد عمران، الالتزام بالإعلام الإلكتروني قبل التعاقد عبر شبكة الانترنت، القاهرة: الدار الجامعي، ٢٠٠٦.
٥. طارق محمد حمزة، النقود الإلكترونية كأحدي وسائل الدفع، بيروت: منشورات زين الحقوقية، ٢٠٠١.

ثانياً- الأبحاث والمجلات والدوريات:

١. أحمد إبراهيم دهشان، "العملات الافتراضية إشكالياتها وأثارها على الاقتصاد المحلي والعالمي"، المؤتمر الدولي الخامس عشر لكلية الشريعة والدراسات الإسلامية، كلية الشريعة جامعة الشارقة، (٢٠١٩): ص ١٢.
٢. أحمد حسن، "الموكلين استخدام الجماعات والمنظمات الإرهابية للتقنيات الافتراضية العملات الافتراضية نموذجاً"، الاتحاد العربي للمكتبات والمعلومات، ع ٣٠، (٢٠٢١): ص ١٤٨.
٣. أحمد سعد على، "العملات الافتراضية المشفرة ماهيتها خصائصها تكيفاتها الفقهية بيتكوين نموذجاً"، مجلة دار الإفتاء المصرية، ع ٣٩، (٢٠١٩): ص ١٣٣.
٤. أحمد قاسم فرج، "العملات الافتراضية في دولة الإمارات العربية المتحدة – الحاجة إلي إطار قانوني لمواجهة مخاطرها، دراسة مقارنة"، بحث منشور في مجلة جامعة الشارقة، العدد ٢، (٢٠٠٩): ص ٧١٣.
٥. أشرف توفيق شمس الدين، "مخاطر العملات الافتراضية في نظر السياسة الجنائية"، مجلة مصر المعاصرة، الجمعية المصرية للاقتصاد السياسي والإحصاء والتشريع، مج ١١٠، ع ٥٣٥، (٢٠١٩): ص ٢٣٧.
٦. جميل عبد الباقي الصغير، "الجرائم الناجمة عن الحاسب الآلي والإنترنت"، المؤتمر الدولي الأول لقانون الإنترنت نحو علاقة قانونية وإدارية واقتصادية وسياسية واجتماعية جديدة - المنظمة العربية للتنمية، (٢٠٠٥): ص ٤٧.

٧. راشد عبد الرحمن أحمد محمد، "العملات الافتراضية ووسائل الدفع الإلكترونية البتكوين نموذجاً"، مجلة العلوم الشرعية جامعة القصيم، مج ١٤ ع ٣، (٢٠٢١): ص ٣١١.
٨. سبتي بن مصيليت سبتي، "العملات الافتراضية دراسة فقهية تأصيلية"، مجلة جامعة الملك عبد العزيز، مج ٢٨، ع ١٢، (٢٠٢٠): ص ٤١٦.
٩. شريف غنام، "محفظة النقود الإلكترونية، رؤية مستقبلية"، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، دبي، (٢٠٠٣): ص ١١٧.

ثالثاً. المراجع الالكترونية:

١. <https://www.youm7.com/story>

٢. <https://groups>

رابعاً. المراجع الأجنبية

1. Alcon, legitimizing Bitcoin ; Policy Recommendations 'Nov.2013
2. DeFiLippi Bitcoin: A Regulatory Nightmare to a Libertarian Dream, Internet Policy Review 2014,3. (٢)
3. Godlove 'Regulatory Overview of virtual currency, oklahoma Journal of law and technology 'Jan.2014, vol,10, Num. 1
4. Kien-Meng Ly, coining Bitcoin's, 'Legal-Bits': Examining the regulatory framework for bitcoin and virtual currencies, Harvard Journal of Law, Technology, Vole .27,Num. 2,spring 2014.