المسؤولية الجنائية عن جرائم غسل الأموال عبر العملات المشفرة

أكرم صالح محمد عرب
طالب باحث بسلك الدكتوراه
تخصص القانون الخاص
تحت إشراف: دة. لطيفة المهداتي
أستاذة التعليم العالي
جامعة محمد الخامس – الرباط
المغرب

الملخص

تُشكّل عمليات غسل الأموال عبر العملات المشفرة حَدثاً عابراً للرقابة المصرفية، مستغلةً تقنية "سلسلة الكتل" وخبيئة "المجهولية" لتمويه العائدات الإجرامية ودمجها في الاقتصاد، وقد أدى هذا التطور الرقمي المتسارع إلى مأزق قانوني يكشف عن عجز القواعد الجنائية التقليدية أمام هذه الأنماط المستحدثة من الجرائم المالية.

وتكمن الإشكالية في مدى ملاءمة القواعد العامة للمسؤولية الجنائية والآليات الإجرائية القائمة للتعامل مع تحديات العملات المشفرة؛ وتتفرع عنها أسئلة حول التكييف الجنائي للأصول الافتراضية، ومسؤولية الفاعلين ومزودي الخدمات، وكفاية آليات التحري والضبط الرقمي لمواجهة هذه الظاهرة.

ولقد اعتمدت الدراسة على المنهج التحليلي النقدي للقواعد القانونية الموضوعية والإجرائية لمكافحة غسل الأموال، والمنهج المقارن لاستعراض التجارب التشريعية والمعايير الدولية كـ((FATF ، إلى جانب المنهج الوصفي لتفكيك الطبيعة التقنية للعملات المشفرة والمحافظ الرقمية.

وخلصت الدراسة إلى وجود ثغرات تشريعية في التكييف القانوني للأصول الرقمية وإسناد المسؤولية للجماعات غير الممركزة، وأكدت أن المواجهة الفعالة تقتضي فرض إلزام تنظيمية صارمة على منصات التداول) كقواعد(KYC ، وتطوير قدرات التحقيق الجنائي الرقمي، واعتماد تدابير تحفظية حاسمة لتجميد ومصادرة المفاتيح الرقمية المشفرة.

الكلمات المفتاح: المسؤولية الجنائية – جرائم غسل الأموال – العملات المشفرة

المقدمة:

تُعد العملات المشفرة واحدة من أبرز تجليات الثورة الرقمية في المجال المالي؛ حيث تعتمد على تقنيات التشفير وسلسلة الكتل (**Blockchain**)لإجراء المعاملات المالية بعيداً عن السلطات المركزية والرقابة المصرفية التقليدية، وقد وفرت هذه التكنولوجيا سرعة فائقة ومرونة عالية في نقل الأموال عبر الحدود، مما جعلها أداة جاذبة للمتعاملين في الاقتصاد الرقمي الحديث.

وبالتوازي مع منافعها الاقتصادية، تنطوي العملات المشفرة على مخاطر جسيمة تنبع أساساً من خبيئة "المجهولية (**Anonymity**) " وصعوبة تتبع هوية أطراف المعاملات، فغياب الوسطاء الماليين التقليديين وتشتت النطاق الجغرافي للشبكات الرقمية يفرضان تحديات غير مسبوقة أمام أجهزة الرقابة والإنفاذ القانوني، مما يحول هذه الأصول إلى ملاذات آمنة محتملة للأنشطة غير المشروعة.

وتُشكل هذه الخصائص الرقمية بيئة خصبة لمرتكبي جرائم غسل الأموال؛ حيث يُستغل الفضاء السيبراني لإجراء مراحل التمويه والدمج للأصول المكتسبة من جرائم أصلية (كالتحايل، والاتجار بالمخدرات، والجرائم السيبرانية)، ويجري تحويل الأموال غير المشروعة إلى رموز رقمية مشفرة، ثم تدويرها عبر منصات وصرافات رقمية متعددة لقطع الصلة بين الجريمة المصرفية ومصدرها الأصلي.

وأمام هذا التطور المتسارع، وجدت القواعد الجنائية التقليدية نفسها أمام مأزق ملموس؛ إذ بنيت أحكام التجريم والرقابة على المفهوم المادي للأموال وعلى الدور المحوري للمؤسسات المصرفية التقليدية، ونتيجة لذلك برزت ثغرات قانونية وتنفيذية في تحديد العناصر المادية والمعنوية للجريمة، وفي معالجة الإسناد الجنائي وصعوبة إثبات القصد الجنائي لدى مستخدمي أو مشغلي هذه المنصات.

وتستدعي هذه المعطيات دراسة المسؤولية الجنائية الناتجة عن استغلال العملات المشفرة في تبييض الأموال، للوقوف على التكييف القانوني الصحيح لهذه الأفعال، ولتقييم مدى كفاية السياسة الجنائية الحديثة في التوفيق بين تشجيع الابتكار التكنولوجي وبين حماية الأمن الاقتصادي والمالي للمجتمع.

وتتبلور الإشكالية المركزية لهذه الدراسة في السؤال الرئيسي التالي:

"إلى أي مدى تستجيب القواعد العامة للمسؤولية الجنائية للتحديات التي تفرضها جرائم غسل الأموال عبر العملات المشفرة، وما هي الآليات التشريعية المعتمدة لمواجهتها؟"

ويتفرع عن هذا السؤال المركزي أسئلة فرعية من قبيل:

- ما هو التكييف القانوني لعملية غسل الأموال باستخدام العملات المشفرة وأركانها الجنائية؟
- كيف تترتب المسؤولية الجنائية للأشخاص الطبيعيين والاعتباريين عن التعامل بالعملات المشفرة المشبوهة؟
- ما هي التدابير الوقائية والتنظيمية فرضتها التشريعات على المنصات والمحافظ الرقمية؟
- ما هي الآليات الإجرائية والجنائية المتبعة لملاحقة وضبط جرائم غسل العملات المشفرة؟

للاجابة عن الاشكالية والأسئلة المتفرعة عنها نقترح خطة تتركب من المحورين الاتيين:

- **المحور الأول: الأطر الموضوعية للمسؤولية الجنائية عن غسل الأموال المشفرة**
- **المحور الثاني: الآليات التنظيمية والإجرائية لمكافحة غسل الأموال المشفرة**

المحور الأول: الأطر الموضوعية للمسؤولية الجنائية عن غسل الأموال المشفرة

يستلزم تنظيم المسؤولية الجنائية عن الأنشطة غير المشروعة في البيئة الرقمية وضع تأصيل موضوعي متين يستوعب الخصائص الفريدة للأصول المشفرة، فالانتقال من المفاهيم القانونية التقليدية للمال والمؤسسة المالية إلى مفاهيم افتراضية غير متمركزة يوجب التثبت أولاً من مدى صلاحية القواعد الجنائية الموضوعية للاحتواء والتطبيق.

وإن دراسة هذا البعد الموضوعي تنقسم بضرورة الحال إلى شقين متكاملين: يتعلق الشق الأول بالبناء المفهومي والجرمي للسلوك المادي والمعنوي لعملية الغسل الرقمي، بينما يتصل الشق الثاني بإسناد هذا السلوك إلى أصحابه وتحديد نطاق المسؤولية الجزائية المترتبة عليه.

وبناءً على ذلك، يتوزع هذا المحور على فقرتين أساسيتين؛ حيث تخصص الفقرة الأولى للبحث في التكييف القانوني والأركان الجنائية لغسل الأموال عبر العملات المشفرة، بينما تعالج الفقرة الثانية نطاق الإسناد الجنائي وأحكام المسؤولية للشخصين الطبيعي والاعتباري.

الفقرة الأولى: التكييف القانوني والأركان الجنائية لغسل الأموال عبر العملات المشفرة

يثير إقحام العملات المشفرة في مسار غسل الأموال إشكالية مدى توافق هذه الوسائط الرقمية مع المفاهيم التقليدية للجريمة؛ إذ يتطلب أمر تجريمها توفيق المفهوم الجنائي لد "مال" مع طبيعة الرموز الافتراضية، فضلاً عن تحديد المظاهر المادية والركن المعنوي للأنشطة المرتكبة.

ومن هنا، يتطلب التحليل الأكاديمي تفكيك الركنين المادي والمعنوي ومعاينة مدى ملاءمة النصوص الجنائية القائمة للتعامل مع هذا النمط المستحدث من الأصول الذكية.

واستناداً إلى ذلك، سنناقش هذه الإشكالية من خلال نقطتين رئيسيتين: أولاً: الطبيعة القانونية للعملات المشفرة وتكيفها كـ "أموال" في جرائم الغسل، وثانياً: الأركان المادية والمعنوية للجريمة في البيئة الرقمية المشفرة.

أولاً: الطبيعة القانونية للعملات المشفرة وتكيفها كـ "أموال" في جرائم الغسل.

تثير العملات المشفرة كـ **Bitcoin** و **Ethereum** جدلاً فقهياً وقانونياً واسعاً بصدد تحديد طبيعتها الذاتية، نظرًا لأنها تتجرّد من الكيان المادي الملموس ولا تستند إلى سلطة إصدار مركزية أو غطاء صريح من الدولة،و يرى جانب من الفقه المالي أن هذه الرموز الافتراضية لا تعدو كونها سلعاً رقمية (**Digital Commodities**) أو قيوداً محاسبية مشفرة تُتداول عبر شبكة الند للند (**P2P**) بناءً على ثقة المتعاملين؛ بينما يتجه رأي آخر إلى اعتبارها وسائل دفع واستثمار بديلة تمتلك وظائف المال التقليدي من حيث التبادل والمقاصة [1]،فهذا التجاذب بين الصفة السلعية والصفة النقدية يلقي بظلاله على مبدأ الشرعية الجنائية، حيث تصطدم السلطات القضائية باستجلاء مدى إمكانية إسباق الحماية الجنائية المقررة للأموال التقليدية على هذه الكيانات الرقمية غير الملموسة.

ومن الناحية الجنائية، تشترط القوانين العقابية وجريمة غسل الأموال على وجه الخصوص أن ينصب الفعل المجرم على "أصل" أو "مال" أو "عائدات" تحصلت من جريمة أصلية، وبتطبيق هذا الشرط، يتبين أن الغالبية العظمى من التشريعات الحديثة اتجهت نحو توسيع المفهوم الجنائي للمال ليشتمل على كافة القيم الاقتصادية والمنافع، سواء كانت مادية أو معنوية، منقولة أو غير منقولة، وسواء تمثلت في سندات خطية أو سجلات رقمية افتراضية[2] ، وبناءً على هذا المفهوم الواسع، فإن العملات المشفرة تُكيف جنائياً على أنها "أموال" أو "ممتلكات افتراضية ذات قيمة اقتصادية"؛ وبالتالي فإن إخفاء مصدرها الناتج عن أفعال جرمية أو تحويلها يقع تحت طائلة تجريم غسل الأموال دون مخالفة لمبدأ التفسير الضيق للنصوص الجنائية.

---

[1] - Teichmann, F., & Falker, M. Cryptocurrencies and Money Laundering: The Regulatory Framework and Beyond. Journal of Financial Crime, 28(4) (2021)., 1120-1134.

[2] – الزوبني، علي جاسم. المواجهة التشريعية لجرائم الأصول الافتراضية والتحديات الإجرائية في تعقبها. دار الفكر الجامعي، الإسكندرية،(2020). ص 84-89.

ويترتب على تكييف العملات المشفرة كأموال افتراضية النفاذ إلى مرحلة البناء القانوني للجريمة الأصلية(**Predicate Offense**) ؛ فالرموز الرقمية المشفرة قد تكون هي بنفسها موضوع الجريمة الأصلية (كالاستيلاء عليها عبر الاختراق السيبراني أو التحايل الرقمي)، أو قد تكون هي الوسيلة والمقابل المالي المباشر لجرائم أصلية أخرى (كالاتجار بالمخدرات عبر الإنترنت المظلم**Dark Web** ، وفي كلا الحالتين، عندما يُعاد تدفق هذه الرموز عبر الصرافات الرقمية أو المحافظ لإخفاء مصدرها الجرمي، يستقر الوصف القانوني للعملات المشفرة باعتبارها "محل الجريمة (**Objectum Delicti**) "في فعل الغسل[3] ، وهذا التحديد يمنح الأجهزة القضائية السند القانوني لتتبع حركة التحويلات الافتراضية وملاحقة وسائطها المالية الذكية.

وحرصت المنظمات الدولية، وفي مقدمتها مجموعة العمل المالي(FATF) ، على حسم هذا اللبس التشريعي عبر إصدار معايير ملزمة تُعرف "الأصول الافتراضية (**Virtual Assets**) "بأنها القيمة الرقمية التي يمكن تداولها أو نقلها أو استخدامها لأغراض الدفع والاستثمار[4] ، وقد انعكس هذا المنظور على التشريعات الوطنية الحديثة التي عدّلت قوانين مكافحة غسل الأموال لتصرح شموليتها للقيم والرموز الرقمية، مما قضى على الثغرات التي كان يستغلها الجناة بالادعاء بأن العملات المشفرة ليست "أموالاً بليغة" بالمعنى القانوني، وفرض بالتالي التزاماً شاملاً بتطبيق أحكام التجريم على كافة أشكال التداول الافتراضي المشبوه.

ثانياً: الأركان المادية والمعنوية للجريمة في البيئة الرقمية المشفرة

يتحقق الركن المادي لجريمة غسل الأموال عبر العملات المشفرة من خلال أي فعل ينطوي على تحويل أو نقل أو إخفاء للأصول الرقمية المتحصلة من جريمة، ولكن بأدوات تقنية حديثة،و تتمايز المظاهر المادية في البيئة المشفرة باستخدام تقنيات خلط العملات (**Coin Mixers/Tumblers**)، والتحويل بين العملات عبر المنصات اللامركزية(**DEXs**) ، أو الاستعانة بـ "عملات الخصوصية " (**Privacy Coins**)مثل **Monero**[5] ،وهذه السلوكيات المادية تُحدث انقطاعاً بين المال المشفر الجرمي ومصدره الأصلي، وتُشكل السلوك المادي المجرم القانوني لقاطعي الصلة المصرفية، حيث يقع الفعل المادي بمجرد إصدار المعاملة الرقمية (**Transaction**) وتأكيدها ضمن سلسلة الكتل(**Blockchain**) .

ويتطلب تمام الركن المادي تحقق النتيجة الإجرامية المتمثلة في إسباغ صبغة المشروعية الزائفة على الأصول المشفرة أو نجاح إخفاء معالمها عن أعين الأجهزة الأمنية والرقابية، وتبرز في هذا الصدد إشكالية "علاقة السببية" الجنائية، حيث تتوزع الأفعال المادية على سلسلة من البرمجيات والأكواد والأطراف المتباعدين جغرافياً عبر العالم [6]، غير أن الاستقرار الفقهي والقضائي يتجه إلتبار أن أي فعل يساهم عمداً في تعقيد مسار التتبع الرقمي أو إدخال الأموال المشبوهة في المحافظ الرقمية يُعد سبباً مباشر أو غير مباشر في تحقق النتيجة الإجرامية، مما يكتمل معه البناء المادي للجريمة.

لقد استلزم التكييف الجنائي لهذه الجريمة توافر القصد الجنائي العام بعنصريه العلم والإرادة لدى الفاعل،و ينبغي أن ينصب علم الجاني على أمر أساسي وهو أن العملات المشفرة التي يتعامل بها أو يحولها تحصلت من مصدر جرمي أو جريمة أصلية، بالإضافة إلى اتجاه إرادته الحرة إلى

---

[3] - King, R., & Clough, J. Crypto-assets, Blockchain and the Limits of Criminal Law: A Comparative Analysis. International Journal of Law and Information Technology, 28(4), . (2020)pp 310-335.

[4] - Financial Action Task Force (FATF). Updated Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers. FATF, Paris, (2021). pp. 12-15.

[5] - Möser, M., Böhme, R., & Breuker, D. An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem. Journal of Cybersecurity and Financial Crime, 12(3), (2018).145-168.

[6] – الشوابكة، باسم. الإجرام السيبراني المالي وأثر تقنيات التشفير على قواعد الإثبات الجنائي. مجلة الدراسات القانونية المقارنة، المجلد 8، العدد 1،(2022). ص 112-115.

إبرام المعاملة الرقمية والتشفيرية[7] ، ويطرح عنصر العلم تحديات إثباتية كبرى في البيئة الرقمية؛ نظراً لسهولة ادعاء الجناة بجهلهم بمصدر الأموال الرقمية أو هويات المتعاملين، مما يدفع النيابات العامة إلى الاستدلال على العلم اليقيني من خلال القرائن القضائية (مثل التداول عبر منصات غير مرخصة، أو استخدام أدوات حجب الهوية، أو نقل المبالغ بأسعار تفوق القيمة السوقية).

ولا يكتفي القانون بوجود القصد العام، بل يشترط توافر قصد جنائي خاص (**Dolus Specialis**) يتمثل في نية الجاني وإرادته المتجهة خصيصاً إلى "إخفاء" أو "تمويه" الطبيعة الحقيقية للأصول المشفرة أو مصدرها أو مكانها أو صاحب الحق فيها، أو إعانة شخص متورط في الجريمة الأصلية على التملص من الآثار القانونية لفعله[8] ، وتتجلى هذه النية الخاصة بوضوح في لجوء المتهم إلى تحويل الأموال عبر عدة محافظ رقمية وهمية في أوقات متقاربة، أو استخدام تقنيات التقسيم المالي (**Structuring**) لتفادي المعايير التنظيمية للإنذار، حيث تشير هذه الآليات التشفيرية المعقدة بذاتها إلى اتجاه النية نحو التعمية والتبييض.

الفقرة الثانية: نطاق الإسناد الجنائي وأحكام المسؤولية للشخصين الطبيعي والاعتباري

يمثل تحديد الشخص المسؤول عن جريمة غسل الأموال المشفرة عقبة رئيسية نظراً لخاصية المجهولية وتداخل أدوار الأطراف الفاعلة بين مستخدمين ومطورين ومنصات تداول رقمية.

ويتطلب تحديد الإسناد الجنائي التمييز بوضوح بين المسؤولية الشخصية المباشرة للأفراد، وبين المسؤولية الجنائية المستقلة أو التبعية للكيانات والشركات المزودة لخدمات الأصول الرقمية.

وعليه، تنقسم هذه الفقرة إلى جزأين متتابعين: أولاً: قيام المسؤولية الجنائية للأشخاص الطبيعيين (المتعاملون والمطورون والوسطاء)، وثانياً: أطر قيام المسؤولية الجنائية للأشخاص الاعتباريين (منصات التداول ومقدمو المحافظ الرقمية.)

أولاً: قيام المسؤولية الجنائية للأشخاص الطبيعيين (المتعاملون والمطورون والوسطاء)

تتأسس المسؤولية الجنائية للأشخاص الطبيعيين في صورتها التقليدية على المباشرة الشخصية للفعل المجرم؛ حيث يُسند الاتهام المباشر لكل فرد يقوم بشراء أو تحويل أو استبدال عملات مشفرة مع علمه أنها متحصلة من مصدر جرمي أو جريمة أصلية، وتتحقق هذه المسؤولية سواء كان المتعامل هو الجاني الأصلي في الجريمة الأولى (كمن يقوم بتبييض أموال سرقها بنفسه عبر هجوم سيبراني)، أو كان شخصاً آخر استعان به التنظيم الإجرامي كـ "وسيط مالي (Money Mule) "مقابل عمولة محددة[9] ، وتكمن الدقة الفقهية هنا في أن الجاني الطبيعي لا يستطيع التذرع بطبيعة المعاملات الرقمية المعقدة لدرء المسؤولية عنه، متى ما ثبت يقينياً اتجاه إرادته الواعية إلى استغلال خاصية التشفير لقطع الصلة بين الأصول المشفرة والمصدر الجرمي الذي نبعت منه.

ويثير تحديد المسئولية الجنائية لمطوري البرمجيات والمشفرين (Developers) جدلاً قانونياً محتدماً في الفقه المعاصر؛ إذ يطرح السؤال حول مدى إمكانية مساءلتهم جزائياً عند استخدام شفراتهم المبرمجة أو تطبيقاتهم اللامركزية (DApps) في غسل الأموال،و يتجه الرأي الفقهي والقضائي الراجح إلى التمحيص بين المطور حسن النية الذي يطلق برمجيات مفتوحة المصدر لأغراض مشروعة، وبين المطور الذي يصمم أدوات تكنولوجية مُعدة خصيصاً وموجهة للتعمية المالية وكسر تتبع الأدلة الجنائية (مثل مجمعات التجميع والتدميج الذاتي Privacy

[7] – العبيدي، محمد حسن. غسل الأموال عبر العملات المشفرة: دراسة مقارنة في القانون الجنائي والتشريعات المالية. مجلة الحقوق والعلوم القانونية، جامعة بغداد، المجلد 15، العدد 2، (2022).ص 201-205.

[8] – شتا، خالد مصطفى. التكوين والتكييف الجنائي للرموز المشفرة في ضوء المعايير الدولية لمكافحة غسل الأموال. المجلة الدولية للدراسات القانونية، القاهرة(2023).، ص 142.

[9] -King, R., & Clough, J. .op.cit .p 310-335.

(Protocol Mixers،[10] ففي الحالة الأخيرة، يرتفع الستار عن المسئولية الشخصية للمطور باعتباره مساهماً أصلياً أو شريكاً بالتسبب عبر تقديم التسهيلات والتجهيزات التقنية اللازمة لإتمام الجريمة مع علمه وإرادته للمآل الإجرامي لبرمجياته.

وتتداخل أشكال المساهمة الجنائية في البيئة الافتراضية نتيجة لتوزع الدور التنفيذي للجريمة بين عدة أطراف عبر العالم، مما يوجب إعمال قواعد الاشتراك والجريمة المنظمة. يُكيف الوسيط الطبيعي الذي يقوم بنقل الأموال أو شراء الأصول الرقمية بطلب من غيره كـ "شريك بالاتفاق أو المساعدة" متى كانت لديه الشبهة الكافية وقبل المخاطرة الجنائية دون التحقق من مشروعية مصدر الأموال[11] ، أما إذا قام الوسيط بإنشاء شبكة من المحافظ وهمية الإدارة وإدارتها بنفسه كجزء من خطة إجرامية محبوكة، فإنه يُكيف حكماً كـ "فاعل أصلي" أو مساهم مباشر في الجريمة المادية؛ مما يستتبع تطبيق العقوبات الأشد المخصصة لجرائم غسل الأموال العابرة للحدود والمنظمة تكنولوجياً.

وتُمثل دفوع "الجهل بالواقع التقني" أو "الوقوع في الغلط" إحدى أبرز الدفوع المقدمة من الأشخاص الطبيعيين لرفع الإسناد الجنائي، حيث يدعي المتهمون غالباً عدم فهمهم لطبيعة شبكات سلسلة الكتل (**Blockchain**) أو جهلهم بالمصدر الجرمي للعملات التي استلموها عبر منصات التبادل،و يقرر الاستقرار القضائي الجنائي أن الجهل بالقواعد التقنية لا يُعد مانعاً من موانع المسؤولية الجنائية أو خطأً مانعاً من العقاب إذا كان بمقدور الشخص الطبيعي التحري والحيطة وفق معيار الشخص المعتاد[12] ، واستناداً إلى ذلك، فإن قبول الأشخاص التعامل بأصول رقمية من جهات غير معروفة أو عبر أسواق غير رسمية دون مبرر مشروعي يُعد قرينة على السلوك الجسيم والمخاطرة المنظمة، مما ينفي ادعاء حسن النية ويُثبت الإسناد الجنائي بحقهم.

ثانياً: أطر قيام المسؤولية الجنائية للأشخاص الاعتباريين (منصات التداول ومقدمو المحافظ الرقمية)

أقرت معظم التشريعات الحديثة والمعايير المالية الدولية إمكانية قيام المسؤولية الجنائية للأشخاص الاعتباريين (كشركات التداول الرقمي، ومزودي المحافظ الحافظة، ومؤسسات الوساطة المادية) عن جرائم غسل الأموال، وتستند هذه المسؤولية إلى فكرة "الخطأ المصلحي" أو "الخطأ التنظيمي"؛ حيث تُساءل الشركة جنائياً إذا ارتكبت الجريمة لحسابها أو باسمها أو بواسطة أحد أجهزتها أو ممثليها الشرعيين[13] ، ولا تتطلب هذه المسؤولية بالضرورة تحديد شخص طبيعي بعينه وإدانته، بل يكفي ثبوت وقوع الفعل المجرم في إطار نشاط الكيان الاعتباري ونتيجة للتغاضي التعمدي أو الفشل الهيكلي في وضع الرقابة المنصوص عليها قانوناً للحد من الأنشطة الإجرامية الافتراضية.

ولا تقتصر مسؤولية منصات التداول ومقدمي المحافظ على المشاركة المباشرة في التمويه، بل تتسع لتشمل الجرائم الواقعة جراء الإهمال التقني والتنظيمي الجسيم(**Gross Organizational Negligence**) ،و تترتب المسؤولية الجنائية أو الإدارية الجزائية على الشركة عند إخفاقها العمدي أو التقصيري الفادح في تطبيق بروتوكولات العناية الواجبة (كالتساهل في تفعيل آليات "عرف عميلك **KYC** "أو الإخفاق في تتبع الأنشطة المالية غير العادية)[14] ،و يُكيف هذا الإخفاق على أنه امتناع مجرم عن القيام بالتزام قانوني فرضه الشارع لحماية النظام العام المالي، مما يجعل الشخص الاعتباري مستحقاً للعقاب الجنائي المستقل عن السلوك الفردي لعملائه.

كماتطرح المنصات اللامركزية (Decentralized Exchanges) والبروتوكولات القائمة على العقود الذكية دون هيئة إدارة ملموسة تحدياً غير مسبوق أمام قواعد المسؤولية الاعتبارية التقليدية؛ نظراً لغياب الممثل القانوني أو المقر الاجتماعي المحدد للشركة،و لمواجهة هذا التفلت التنظيمي، اتجه الفقه والقضاء الحديث إلى تتبع الكيانات الحاكمة الواقعية لهذه البروتوكولات، مثل المنظمات المستقلة اللامركزية (**DAOs**)

---

[10]- Möser, M., Böhme, R., & Breuker, D. .op.cit .p 145-168.

[11] ا-لشوابكة، باسم. م.س.ص 118-122.

[12] -الزويني، علي جاسم.م.س. ص 134-138.

[13] -Teichmann, F., & Falker, .op.cit .p 1120-1134.

[14]- Financial Action Task Force (FATF). .op.cit . pp. 35-40.

أو حائزي رموز الحوكمة (**Governance Tokens**) الذين يمتلكون سلطة التعديل والسيطرة على الشفرة[15] ، وتتيح هذه المقاربة القانونية الحديثة اختراق الحجاب الافتراضي للكيان اللامركزي وإسباق صفة "الشخص الاعتباري الواقعي" عليه، أو مساءلة المؤسسين الحقيقيين بصفتهم منظمة اعتبارية غير مسجلة ارتكبت أفعالاً ضارة بالنظام العام.

وتتميز العقوبات الجنائية المقررة للأشخاص الاعتباريين بطبيعتها الخاصة المقترنة بالطبيعة المادية والمالية للكيانات المعنوية، نظراً لاستحالة إيقاع العقوبات السالبة للحرية عليها مباشرة، وتتدرج هذه الجزاءات من الغرامات المالية المشددة – التي تُحسب غالباً كنسبة مئوية من حجم المعاملات أو الأصول الرقمية المنفذة – وصولاً إلى عقوبات سالبة للحقوق الكلية مثل مصادرة كافة الأصول والرموز المشفرة المملوكة للشركة، أو غلق المقرات الرقمية والسيرفرات، وإلغاء تراخيص التشغيل والإنهاء القانوني للكيان الاعتباري (الحل القضائي)[16] ، وتكفل هذه العقوبات الرادعة إعادة ضبط السوق الرقمي وفرض التزام صارم بالمعايير الرقابية الدولية على كافة الكيانات العاملة في بيئة التشفير.

المحور الثاني: الآليات التنظيمية والإجرائية لمكافحة غسل الأموال المشفرة

لا تكتمل المواجهة القانونية لجرائم غسل الأموال المشفرة بالوقوف عند الأحكام الموضوعية والإسناد الجنائي فقط، بل تقتضي إيجاد آليات إجرائية وتنظيمية تتناسب مع السرعة العابرة للحدود التي تتميز بها حركة الأصول الرقمية.

وتتداخل في هذا الصدد الجهود الوقائية المتمثلة في وضع التزامات تنظيمية صارمة على عاتق الفاعلين في سوق التشفير، مع آليات التحقيق الجنائي القادرة على اختراق جدار التشفير وضبط ومصادرة عائدات الجريمة.

ولأجل ذلك، يتناول هذا المحور موضوع مكافحة الغسل الرقمي عبر فقرتين متكاملتين؛ تُعنى الفقرة الأولى بالتدابير الوقائية والالتزامات التنظيمية على مقدمي الخدمات الرقمية، بينما تُركز الفقرة الثانية على تحديات التحقيق والتتبع الإجرائي للعملات المشفرة وتجميدها.

الفقرة الأولى: التدابير الوقائية والالتزامات التنظيمية على مقدمي الخدمات الرقمية

تُشكل الوقاية الاستباقية خط الدفاع الأول للحد من استغلال الفضاء الافتراضي في تبييض الأموال، عن طريق نقل جزء من العبء الرقابي إلى مقدمي خدمات الأصول المشفرة(**VASPs**) .

وتتجسد هذه الرقابة الوقائية في إلزام المنصات والمحافظ بتدابير العناية الواجبة وإيجاد قواعد موحدة للشفافية والإبلاغ المباشر عن أي معاملات تشوبها الشبهة.

وبناءً عليه، سنبحث هذه الالتزامات من خلال عنصرين هما: أولاً: تطبيق قواعد "عرف عميلك (KYC) "والعناية الواجبة في منصات التداول، وثانياً: التزام مقدمي أصول التشفير بالإبلاغ عن المعاملات المالية المشبوهة.

أولاً: تطبيق قواعد "عرف عميلك (KYC) "والعناية الواجبة في منصات التداول.

تُمثل قواعد "عرف عميلك (**Know Your Customer – KYC**) "والتدابير التابعة لها ضمن إطار "العناية الواجبة تجاه العملاء (**Customer Due Diligence - CDD**) "خط الدفاع التنظيمي الأول لمنع نفاذ الأموال غير المشروعة إلى أسواق التداول المشفرة،و يفرض هذا الالتزام على منصات التداول ومزودي الخدمات الرقمية التحقق النظري والفني المباشر من الهوية الحقيقية للمستخدمين قبل إتاحة فتح المحافظ الافتراضية أو تنفيذ عمليات التبادل[17] ، ولا ينحصر هذا الواجب عند مجرد جمع البيانات الشخصية

[15] –شتا، خالد مصطفى. م.س. ص 160-165.

[16] –العبيدي، محمد حسن. م.س.ص 225-230.

[17] – Financial Action Task Force (FATF). .op.cit . pp. 22-28.

التقليدية (كبطاقات الهوية وعناوين الإقامة)، بل يمتد لفرز ومطابقة تلك البيانات مع قواعد البيانات الجنائية وقوائم العقوبات الدولية، للحيلولة دون استخدام الفضاء السيبراني كملاذ لغاسلي الأموال والمتهربين من الملاحقات القضائية.

وتأخُذ تدابير العناية الواجبة في مجال العملات المشفرة نموذجاً مرناً يُعرف بـ "النهج القائم على المخاطر (**Risk-Based Approach**)"، حيث تتدرج المنصات في إجراءات التحقق وفقاً لطبيعة العملية وحجمها ونوع الأصول الرقمية المستعملة. تتراوح هذه الإجراءات بين "العناية العادية" للعمليات المألوفة ذات الأحجام المحدودة، و"العناية المشددة (**Enhanced Due Diligence – EDD**)" عند التعامل مع أشخاص ممكّنين سياسياً(**PEPs**) ، أو عند تنشيط معاملات تتضمن "عملات خصوصية" عالية التشفير، أو التحويل من وإلى نطاقات جغرافية عالية المخاطر [18]،و يترتب على هذا التدرج التزام المنصات بالتثبت من المصدر الأصلي للثروة الرقمية للعميل وفحص الغرض الاقتصادي من المعاملة قبل إتمامها قانونياً.

وتواجه منصات التداول عقبات تقنية معقدة أثناء إنفاذ قواعد "عرف عميلك"، نتيجة لتطور أساليب التزوير الرقمي والانتحال في العالم الافتراضي. يلجأ غاسلو الأموال إلى استخدام مستندات هوية مزيفة يتم إنشاؤها عبر الذكاء الاصطناعي(**Deepfakes**) ، أو الاستعانة بروابط وشبكات وهمية (**Proxies/VPNs**) لتضليل نظام الموقع الجغرافي الخاص بالمنصة[19] ، وتفرض هذه التكتيكات الإجرامية على المؤسسات الرقمية الاستثمار في تقنيات "التحقق البيومتري المتقدم" وآليات المطابقة الفورية عبر سلسلة الكتل، لإحباط محاولات إنشاء المحافظ المجهولة أو استغلال ثغرات التسجيل السريع التي تُضعف القيمة القانونية لعمليات التثبت الرقمي.

ويُرتب القانون آثاراً زجرية وتنظيمية صارمة على منصات التداول الرقمي التي تتهاون أو تمتنع عن تطبيق بروتوكولات العناية الواجبة تجاه العملاء،و لا يقتصر الأثر على سحب ترخيص التشغيل وإدراج الكيان المالي ضمن القوائم السوداء للمؤسسات الرقابية فحسب، بل يمتد للوصول إلى التجريم المباشر لمجلس إدارة المنصة أو مسؤولي الامتثال (**Compliance Officers**) بتهمة الامتناع المجرم والإهمال الجسيم في الحفاظ على أمن المعاملات المالية[20] ،و الشارع القانوني ينظر إلى قواعد "عرف عميلك" باعتبارها التزاماً بحقق وليس مجرد بذل عناية، مما تجعل أي إخلال بها سبباً مباشراً لقيام المسؤولية الإدارية والجزائية الشاملة ضد الكيان الاعتباري وممثليه.

ثانياً: التزام مقدمي أصول التشفير بالإبلاغ عن المعاملات المالية المشبوهة

يُعد التزام مقدمي خدمات الأصول المشفرة (**VASPs**) بالإبلاغ عن المعاملات المشبوهة تكليفاً آتيّاً يستهدف تحويل تلك الكيانات الافتراضية إلى عين رقابية لصالح وحدات التحريات المالية الوطنية(FIUs) ،و يتأسس هذا الالتزام على قاعدة الحماية الاستباقية للأسواق؛ حيث يُلزم القانون إدارة المنصة بمجرد اكتشاف أي مؤشر على معاملة غير مبررة أو نمط تحويل غير معتاد بالإخطار الفوري للجهات المختصة دون حاجة للتثبت القطعي من وجود الجريمة الأصلية[21] ، ويعفى المبلغون حسن النية من أي مسؤولية مدنية أو جنائية أو عقدية ناتجة عن إفشاء السرية المهنية أو تأخير تنفيذ المعاملات، مما يقوي الحافز الرقابي لدى المنصات للتعاون مع جهات الإنفاذ القانوني.

وتستند عمليات الكشف والإبلاغ إلى جملة من "مؤشرات الشبهة (**Red Flags**)" التي تم تطويرها توافقاً مع المعايير الدولية لمكافحة الغسل الرقمي،و تبرز من بين هذه المؤشرات: إجراء تحويلات مكثفة ومتقاطعة لمبالغ تجزئية تفادياً لسنن الإفصاح المالي(**Structuring**) ، أو توجيه التحويلات فجأة إلى محافظ مرابطة بأسواق الإنترنت المظلم(**Darknet Markets**) ، أو استخدام الأدوات المسماة خالي

[18] -Teichmann, F., & Falker, M. op.cit .p 1120-1134.

[19] -الشوابكة، باسم. م.س.ص 130-134.

[20] -العبيدي، محمد حسن. م.س. ص 240-245.

[21] -الزوبني، علي جاسم.م.س.ص 162-167.

الطبع (**Tumblers/Mixers**) المخصصة لتعمية مسار المعاملة[22]،و تُشكل هذه أنماط السلوك المالي المستهدف بالبحر الرقابي الداخلي للمنصة قرائن قوية توجب إحالة ملف المعاملة والبيانات الرقمية الخاصة بها إلى السلطات المختصة فور استشعار الريبة.

كما تُشكل "قاعدة السفر (**Travel Rule**) "الإطار الأكثر حزامة لإنفاذ التزام الإبلاغ، حيث تلزم التشريعات المتقدمة مقدمي خدمات الأصول الرقمية بضرورة الحصول على بيانات المرسِل والمرسَل إليه وتبادلها وحفظها مع كل تحويل مالي مشفر يتجاوز نصاباً مالياً معيناً[23]،و يهدف هذا الإجراء التقني المشترك إلى ضمان عدم انقطاع "سلسلة التتبع" عند انتقال الأموال بين منصات متواجدة في دول مختلفة، مما يمنع خلق الثغرات التنظيمية العابرة للحدود وتسهيل مهمة أجهزة الاستخبار المالي في ربط البيانات المشبوهة وتحديد النقطة الرقمية التي شابتها عملية التبييض.

و يُحيط الشارع عملية الإبلاغ عن الشبهات بسياج شديد من الكتمان والسرية؛ إذ يحرّم تحريماً قاطعاً ما يُعرف بـ "إفشاء أسرار التحريات " (**Tipping–Off**)، وهو قيام المنصة أو أحد موظفيها بإخطار العميل المشتبه فيه بأن معملاته أصبحت محل إبلاغ أو فحص قضائي[24] ،و يُعد هذا الإفشاء جريمة جنائية قائمة بذاتها تُعرض مرتكبها العقوبات سالبة للحرية وغرامات مشددة، لما يسببه من إضرار بسير التحقيقات وتمكين الجناة من إخفاء مفاتيح التشفير أو تهريب الأصول الرقمية، وفي المقابل يُكيف الامتناع العمدي عن تقديم التقارير المالية المشبوهة كجناية مساهمة بالامتناع في جريمة غسل الأموال نفسها .

الفقرة الثانية: تحديات التحقيق والتتبع الإجرائي للعملات المشفرة وتجميدها

تصطدم قواعد التحقيق الجنائي التقليدية بعقبات تقنية متعددة عند التعامل مع معطيات "سلسلة الكتل"، مما يجعل جمع الأدلة الرقمية وتعقب حركة الأموال المشفرة أمراً في غاية التعقيد.

وتفرض هذه الإشكاليات تطوير آليات البحث الجنائي الرقمي، واستحداث تدابير تحفظية حاسمة تتيح للجهات القضائية والضبطية السيطرة على المفاتيح الخاصة وتجميد الأصول المشفرة ومصادرتها.

وتنفيذاً لذلك، تُقسم هذه الفقرة إلى نقطتين رئيسيتين: أولاً: صعوبات التتبع الجنائي الرقمي وآليات التحري في أدلة "سلسلة الكتل"، وثانياً: الإجراءات التحفظية المتعلقة بتجميد ومصادرة الأصول والتشفيرات الرقمية.

أولاً: صعوبات التتبع الجنائي الرقمي وآليات التحري في أدلة "سلسلة الكتل."

تصطدم سلطات التحقيق الجنائي بعقبات تكنولوجية معقدة عند محاولة تتبع حركة العملات المشفرة، تنبع بالأساس من طبيعة التشفير الذاتي وخاصية "المجهولية المستعارة(Pseudonymity) "، فبالرغم من أن دفتر الموازنة المعمم لسلسلة الكتل (Blockchain Ledger)يسجل كافة المعاملات المالية بصورة علنية وشفافة، إلا أن هذه المعاملات ترتبط بأرقام عناوين ومحافظ رقمية مشفرة بدلاً من الأسماء الحقيقية لأصحابها[25] ،وتتفاقم هذه العقبة التقنية مع لجوء المتهمين إلى إنتاج عناوين رقمية متغيرة مع كل معاملة جديدة، أو الاعتماد على شبكات التشفير المتقدمة والمعاملات الخارجية عن سلسلة الكتل(Off-Chain Transactions) ، مما يقطع تسلسل الأدلة الجنائية ويحول دون ربط العنوان الرقمي بالهوية المادية لمرتكب الجريمة.

---

[22] -Möser, M., Böhme, R., & Breuker, D. An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem. Journal of Cybersecurity and Financial Crime. (2018), 12(3), 145-168.

[23] -King, R., & Clough, J. op.cit .p 310-335.

[24] -شتا، خالد مصطفى. م.س. ص 175-180.

[25] -King, R., & Clough, J. op.cit .p 310-335.

وتتجاوز صعوبات التحقيق مجرد المجهولية الهيكلية لتمتد إلى الاستخدام المتزايد لأدوات التمويه والتعتيم الرقمي المصممة خصيصاً لإحباط جهود التحري الجنائي. يستعين غاسلو الأموال بتقنيات خلط العملات (Coin Mixers/Tumblers) التي تقوم بتجميع الأصول المشفرة القادمة من مصادر مختلفة وإعادة إرسالها مجزأة إلى عناوين جديدة بعد خلطها، أو التداول عبر "عملات الخصوصية (Privacy Coins)" مثل Monero و Zcashالتي تُخفي تلقائياً قيم المعاملات وعناوين أطرافها[26] ، فهذه الأساليب التمويهية تخلق جداراً تقنياً يُعطل قدرة المحققين التقليديين على إثبات وحدة المصدر والرابطة العليّة بين الأموال المغسولة والسلوك الجرمي الأصلي.

ولمواجهة هذه العقبات التقنية، طوّرت أجهزة إنفاذ القانون آليات تحرٍ حديثة تعتمد على برمجيات الاستخبار الجنائي المخصصة لتحليل سلسلة الكتل(Blockchain Forensics Tools) ،و تعتمد هذه الآليات على خوارزميات التجميع (Clustering Algorithms)والذكاء الاصطناعي لتتبع تدفق النقاط الرقمية، وتحليل أنماط المعاملات المالية عبر الشبكة، وتحديد نقاط التقاء المحافظ الافتراضية مع منصات التداول المركزية التي تطبق قواعد التثبت من الهوية[27] ، وتُشكل هذه الآليات المتقدمة الركيزة الأساسية لاستخلاص "الدليل الرقمي" القابل للاحتجاج به أمام القضاء الجنائي، من خلال ربط العنوان الافتراضي المشبوه بالنقطة المادية التي تم فيها تحويل العملات المشفرة إلى نقد تقليدي.

ونظرًا لأن الشبكات الرقمية لا تعترف بالحدود الجغرافية أو السيادة الإقليمية، فإن جهود التحري والتتبع المحلي تظل قاصرة ما لم تُدعم بمنظومة تعاون قضائي دولي سريعة وفعالة،و يواجه سلطات التحقيق بطئاً إجرائياً في تفعيل الإنابات القضائية الدولية واسترداد البيانات المالية الرقمية من سيرفرات الشركات المتواجدة في الملاذات الآمنة أو الملاذات السيبرانية (**Cyber Havens**) ،[28] واستناداً إلى ذلك، تتجه السياسات الجنائية المتقدمة إلى تفعيل شبكات التواصل الأمني المباشر (مثل شبكة 7/24 التابعة للانتربول) وتبادل المساعدات القانونية المتبادلة (MLA) بآليات فورية، لضمان ملاحقة الأصول الافتراضية المهربة قبل إعادة تدويرها أو إخفائها نهائياً.

ثانياً: الإجراءات التحفظية المتعلقة بتجميد ومصادرة الأصول والتشفيرات الرقمية

يُقصد بالتجميد الإجرائي للعملات المشفرة فرض حظر مؤقت على نقل أو تحويل أو تصرف في الأصول الرقمية المشتبه في اتصالها بجريمة غسل أموال، بناءً على أمر صادر من السلطة القضائية المختصة،و يثير هذا الإجراء إشكالية قانونية تتمثل في كيفية تطبيق مفهوم "الضبط المادي" التقليدي على أصول لا توجد إلا في شكل شفرات برمجية غير ملموسة[29] ، ويتجه الفقه والقضاء الحديث إلى تكييف التجميد الرقمي على أنه "منع إجرائي للوصول إلى الشبكة" يتم تنفيذه إما عبر إلزام منصات التداول المركزية بحظر المحفظة المعنية، أو من خلال السيطرة الفنية الجبرية على المفاتيح الخاصة (Private Keys) التي تُتيح وحدها حق التصرف في الأموال المشفرة.

وتتطلب المباشرة الفعلية لقرارات الضبط والتجميد قدرة سلطات إنفاذ القانون على وضع يدها على المفاتيح الخاصة أو "عبارات الاسترداد (Seed Phrases)"التي تمثل السند الحصري للملكية الرقمية. تتنوع الوسائل الإجرائية بين الضبط المادي للمعدات الإلكترونية والمحافظ الصلبة (Hardware Wallets) أثناء التفتيش القضائي، وبين إعمال قرارات الإلزام القضائي الموجهة للمتهم أو للغير لإفشاء شفرات التشفير تحت طائلة عقوبة الامتناع عن تنفيذ الأوامر القضائية[30] ، وفي حالة المحافظ الحافظة (Custodial Wallets) التابعة لمنصات التداول، يتم التنفيذ الجبري بطلب رسمي موجّه إلى المنصة لنقل الأصول الرقمية المجمّدة إلى محفظة مشفرة تحت الإدارة الحصرية للعدالة.

---

[26] -Möser, M., Böhme, R., & Breuker, D. op.cit .p 145-168.

[27] -الشوابكة، باسم. م.س. ص 140-145.

[28] Financial Action Task Force (FATF). op.cit . pp. 48-52.

[29] الزويني، علي جاسم.م.س. ص 180-185

[30] -Teichmann, F., & Falker, M. .op.cit .p 1120-1134.

وتُعد المصادرة الجنائية الأثر النهائي للإجراءات التحفظية، حيث تقضي المحكمة بنقل ملكية العملات المشفرة المغسولة أو الأدوات المستخدمة في الجريمة إلى ملكية الدولة. ونظراً لخاصية التقلب الشديد في أسعار العملات الرقمية(Volatility) ، تبرز إشكالية إدارة الأصول المصادرة أثناء فترة النزاع القضائي لتفادي فقدان قيمتها الاقتصادية[31] ، واستجابة لذلك أوجدت التشريعات الحديثة قواعد خاصة تتيح للسلطات القضائية بيع الأصول الرقمية المجمّدة بالأسعار السوقية السائدة وتجميد المقابل النقدي التقليدي لحين صدور حكم بات، أو استخدام حسابات وأدوات حراسة رقمية أمينة تُدار عبر مؤسسات مالية مرخصة.

لقد حرص الشارع الجنائي على الموازنة بين مقتضيات الملاحقة الزجرية لجرائم غسل الأموال المشفرة وبين ضرورة كفالة الحماية التشريعية لحقوق الغير حسن النية،و تتجلى هذه الحماية في إتاحة الحق لأطراف المعاملات الرقمية الذين تعاملوا مع المحافظ المجمّدة دون علمهم بمصدرها الجرمي لتقديم الاعتراضات القضائية وإثبات مشروعية شرائهم للعملات أو تقديمهم لخدمات مقابلها [32]، ويتطلب قبول هذا الدفع تقديم أدلة رقمية قاطعة تثبت استيفاء العميل لتدابير التحقق الممكنة وعدم وجود أي مؤشرات شبهة مالية أثناء إجراء المعاملة، مما يستوجب استبعاد حصته المالية من حقل المصادرة وإعادتها لحوزته القانونية.

الخاتمة

توصلت هذه الدراسة إلى أن جرائم غسل الأموال عبر العملات المشفرة تمثل نمطاً ممتداً وغير تقليدي من الجرائم السيبرانية المالية، حيث تُستغل خصائص التشفير والمجهولية لتجاوز المنظومات المصرفية الرسمية، وقد أثبت التحليل القانوني أن القواعد الموضوعية التقليدية للمسؤولية الجنائية – رغم مرونتها – ما زالت تواجه ثغرات في استيعاب الطبيعة القانونية للاقتصاد الرقمي غير المركزي، لا سيما فيما يتعلق بالتكييف الدقيق للأصول المشفرة وإسناد المسؤولية للكيانات الافتراضية غير الممركزة(**DeFi**) .

كما كشفت النتائج أن النجاح في الحد من هذه الجرائم لا يتوقف على تجريم السلوكيات المادية لعمليات التمويه والدمج فحسب، بل يعتمد بدرجة أساسية على صرامة التدابير الوقائية المفروضة على مقدمي خدمات الأصول المشفرة(**VASPs**) ،و تفعيل أدوات الشفافية، مثل قواعد العناية الواجبة وتتبع حركة المعاملات المشبوهة عبر الكتل الرقمية، يمثل الحجر الزاوية في تجريد هذه الوسائل من ميزتها الرئيسية المتمثلة في المجهولية والمخاتلة المالية.

وتأسيساً على ما تقدم، نوصي بالمسارعة إلى تحديث المنظومة التشريعية الجنائية والإجرائية من خلال نص صريح يعترف بالأصول المشفرة كأدوات مالية خاضعة لأحكام ومصادرة تبيض الأموال، مع تطوير القدرات الفنية لمؤسسات إنفاذ القانون في مجال التحليل الجنائي لسلسلة الكتل(**Blockchain Forensics**) ، كما نشدد على أهمية تعزيز التعاون القضائي والأمني العابر للحدود وتوحيد المعايير التنظيمية، لضمان سد المنافذ والتغلب على السيادة الإقليمية المستغلة في الجرائم الرقمية.

[31] –العبيدي، محمد حسن.م.س. ص 255–260.

[32] شتا، خالد مصطفى. م.س.ص 190–194.

المراجع والمصادر:

أولاً: المراجع العربية

- أبو الليل، إبراهيم" المسؤولية الجنائية عن الجرائم السيبرانية وحماية الاقتصاد الرقمي" دار النهضة العربية، القاهرة (2021).
- العبيدي، محمد حسن" غسل الأموال عبر العملات المشفرة: دراسة مقارنة في القانون الجنائي والتشريعات المالية" مجلة الحقوق والعلوم القانونية، جامعة بغداد، المجلد 15، العدد 2، (2022).
- الزويني، علي جاسم" المواجهة التشريعية لجرائم الأصول الافتراضية والتحديات الإجرائية في تعقبها" دار الفكر الجامعي، الإسكندرية (2020).
- شتا، خالد مصطفى" التكوين والتكييف الجنائي للرموز المشفرة في ضوء المعايير الدولية لمكافحة غسل الأموال" المجلة الدولية للدراسات القانونية، القاهرة، (2023).

ثانياً: المراجع الأجنبية

- Financial Action Task Force (FATF). Updated Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers. FATF, Paris. (2021).
- Möser, M., Böhme, R., & Breuker, D. An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem. Journal of Cybersecurity and Financial Crime, 12(3), 145-168. (2018).
- King, R., & Clough, J. Crypto-assets, Blockchain and the Limits of Criminal Law: A Comparative Analysis. International Journal of Law and Information Technology, 28(4), 310-335. (2020).
- Teichmann, F., & Falker, M. Cryptocurrencies and Money Laundering: The Regulatory Framework and Beyond. Journal of Financial Crime, 28(4), 1120-1134. (2021).