المجلة الجزائرية للسياسة والأمن
ISSN: 2800-1095

المجلد: 05 – العدد: 01 - جوان 2026
/ ص.ص 203- 218

الجرائم المالية الرقمية: غسل الأموال عبر العملات المشفرة وبطاقات الدفع الإلكتروني

Digital Financial Crimes: Money Laundering through Cryptocurrencies and Electronic Payment Cards

يمينة حناش [1]*

[1]جامعة قسنطينة3- صالح بوبنيدر، (الجزائر)،
yamina.hannache@univ-constantine3.dz

تاريخ الاستلام: 2026-05-16 **تاريخ القبول:** 2026-06-28 **تاريخ النشر:** 2026-07-10

الملخص باللغة العربية:

تستكشف هذه الورقة البحثية ظاهرة غسل الأموال في البيئات المالية الرقمية، مع التركيز على آليتين متسارعتي النمو: العملات المشفرة وبطاقات الدفع الإلكتروني. واعتمد البحث منهجاً وصفياً تحليلياً لاستقصاء الثغرات التقنية والقانونية التي تتيح استغلال المنصات الرقمية في تبييض العائدات غير المشروعة. وتخلص الدراسة إلى أن اللامركزية التقنية، وسرعة التحويلات العابرة للحدود، وتعدد قنوات الدفع الإلكتروني، تضعف فعالية آليات المراقبة التقليدية، مما يستدعي تحديث الأطر التنظيمية، وتبني حلول تحليلية قائمة على الذكاء الاصطناعي وسلاسل الكتل، وتعزيز التعاون المؤسسي العابر للحدود، بما يرسخ منظومة رقابية استباقية قادرة على مواكبة التطور المالي الرقمي وضبط تدفقات الأموال غير المشروعة بفاعلية.

الكلمات المفتاحية: غسل الأموال الرقمي، العملات المشفرة، الامتثال الرقمي، بطاقات الدفع الإلكتروني، الأطر التنظيمية.

* **المؤلف المرسل**

Abstract:
This research paper explores the phenomenon of money laundering in digital financial environments, focusing on two rapidly expanding mechanisms: cryptocurrencies and electronic payment cards. Employing a descriptive-analytical approach, the study investigates the technical and regulatory vulnerabilities that enable digital platforms to be exploited for laundering illicit proceeds. The findings indicate that technical decentralization, the speed of cross-border transactions, and the proliferation of digital payment channels significantly weaken traditional monitoring mechanisms. Consequently, the study calls for modernizing regulatory frameworks, integrating AI- and blockchain-based analytical solutions, and strengthening cross-border institutional cooperation to establish a proactive regulatory system capable of adapting to digital financial innovations while effectively curbing illicit financial flows.
Keywords: Digital Money Laundering, Cryptocurrencies, Digital Compliance, Electronic Payment Cards, Regulatory Frameworks.

مقدمة:

أدى التسارع غير المسبوق في التحول الرقمي بالقطاع المالي إلى إعادة هندسة المشهد الإجرامي الاقتصادي بشكل جذري، حيث انتقلت عمليات غسل الأموال من المسارات المصرفية التقليدية المعقدة إلى فضاءات رقمية افتراضية تتسم بالمرونة العالية. وتتيح هذه البيئات الإلكترونية الجديدة آليات متطورة لإخفاء الهويات الرقمية، وتجاوز الرقابة الجغرافية والقضائية، وتسريع دورة تبييض العائدات غير المشروعة عبر قنوات يصعب رصدها بالأنظمة الإشرافية التقليدية. كما يسهل الاعتماد المتزايد على البنى التحتية الرقمية الحديثة تفكيك الحواجز الزمنية والمكانية التي كانت تعيق سابقا تنفيذ العمليات المالية المشبوهة على نطاق واسع.

وتبرز العملات المشفرة وأنظمة الدفع الإلكتروني كأدوات محورية تستغلها الشبكات الإجرامية الحديثة، نظرا لطبيعتها اللامركزية، وسهولة الوصول إليها، وانعدام

الإشراف المباشر على شريحة واسعة من معاملاتها العابرة للحدود. وتوظف هذه الأدوات تقنيات تشفير متقدمة وبروتوكولات تحويل سريعة تتيح تجزئة المبالغ الكبيرة إلى تحويلات صغيرة ومتكررة، مما يصعب عملية تتبع المصدر الأصلي للأموال ويضعف فعالية آليات الرقابة المصرفية المعتمدة. ويضاف إلى ذلك استغلال ثغرات المصادقة في المعاملات غير المباشرة، والتي تفتح مسارات موازية لدمج العائدات غير المشروعة في الدورة الاقتصادية الرسمية دون إثارة الشكوك الرقابية.

وفي المقابل، تواجه الهيئات الرقابية والمؤسسات المصرفية تحديات هيكلية ومعرفية متزايدة في محاولة تتبع التدفقات المالية المشبوهة، وفرض معايير الامتثال المالي الموحدة داخل بيئة تتسم بالتسارع الابتكاري والتعقيد التقني. ويعزى هذا القصور الإشرافي إلى التباين الواضح في التشريعات الوطنية، وبطء تحديث خوارزميات كشف الشذوذ السلوكي، وعدم مواكبة الأطر التنظيمية للابتكارات المالية الناشئة التي تعمل خارج النطاق المصرفي التقليدي. كما يخلق غياب آليات التبادل المعلوماتي الفوري بين الدول مساحات تنظيمية رمادية، تستغل من قبل الجناة الماليين للإفلات من المراقبة وتحويل العائدات غير المشروعة عبر سلاسل معقدة يصعب فك تشابكها.

وفي ضوء هذه التحولات الهيكلية والتحديات الرقابية المتشابكة، تبرز الحاجة الملحة إلى إعادة قراءة منهجية للآليات الإشرافية الراهنة، مما يطرح الإشكالية البحثية على النحو التالي: ما هي الآليات التقنية والثغرات التنظيمية التي تمكن من استغلال العملات المشفرة وبطاقات الدفع الإلكتروني في عمليات غسل الأموال، وكيف يمكن تصميم أطر رقابية متكاملة تواكب ديناميكيات الابتكار المالي دون إعاقة مسار التطور التكنولوجي المشروع؟

وانطلاقا من الإشكالية البحثية المطروحة، يمكن صياغة الفرضيات التالية:

- تزداد قدرة الشبكات الإجرامية على استغلال العملات المشفرة وبطاقات الدفع في غسل الأموال طردا مع تعقيد التشفير ودرجة اللامركزية، مما يستدعي تطوير أدوات تحليل جنائي رقمي متقدمة تعوض قصور آليات التتبع التقليدية.

- يسهم التباين التشريعي وغياب التبادل المعلوماتي الآني في خلق مساحات تنظيمية رمادية تستغل للتبييض العابر للحدود، مما يفرض مواءمة الأطر الوطنية مع المعايير الدولية لضمان فعالية الرقابة المشتركة.

- يتحقق بناء أطر رقابية مستدامة من خلال دمج الذكاء الاصطناعي وتحليل سلاسل الكتل مع معايير امتثال مرنة، شريطة تعزيز الشراكات المؤسسية لتحقيق التوازن بين الرقابة الفعّالة والابتكار المالي المشروع.

كما يسعى هذا البحث إلى تحقيق مجموعة من الأهداف، أهمها:

- تفكيك الأدوات التقنية والتنظيمية المُستغلة في تبييض العائدات غير المشروعة عبر الفضاءات الرقمية.

- قياس فاعلية التشريعات والأنظمة الرقابية الراهنة في مواكبة التعقيدات الرقمية المستجدة.

- صياغة مقترحات عملية لآليات رقابية وتقنية تعزز الشفافية المالية وتوازن بين الرقابة والابتكار..

ولتحقيق هذه الأهداف المتكاملة، يعتمد البحث على المنهج الوصفي التحليلي كأداة منهجية رئيسية، حيث يوظف مراجعة نقدية للأدبيات الأكاديمية المحكمة، والتقارير المؤسسية الدولية، والوثائق التنظيمية المعتمدة.

وللإجابة على الاشكالية السابقة، تم تقسيم هذه الورقة البحثية إلى ثلاثة مباحث رئيسية، بالإضافة إلى مقدمة والخاتمة:

المبحث الأول: الإطار المفاهيمي والتنظيمي لغسل الأموال الرقمي.

المبحث الثاني: آليات غسل الأموال عبر العملات المشفرة.

المبحث الثالث: استغلال بطاقات الدفع الإلكتروني في العمليات المالية غير المشروعة.

المبحث الأول: الإطار المفاهيمي والتنظيمي لغسل الأموال الرقمي

يشكل الفهم الدقيق للمفاهيم المالية الرقمية وتطور الأطر القانونية المنظمة لها المدخل الأساسي لمعالجة ظاهرة التبييض الإلكتروني. فقد انتقل التركيز الرقابي من مراقبة المؤسسات المالية التقليدية إلى متابعة المنصات اللامركزية، وشركات التقنية المالية، ومقدمي خدمات الأصول الافتراضية، في ظل تحديات تشريعية وتقنية متشابكة.

المطلب الأول: تطور مفهوم غسل الأموال في العصر الرقمي

لم يعد غسل الأموال مقتصرا على المراحل الكلاسيكية المعروفة، بل تحول إلى عملية رقمية متكاملة تعتمد على تقنيات التشفير المتقدمة، والمحافظ الإلكترونية، والتحويلات الفورية التي تفلت من الرقابة المصرفية المباشرة. وقد توسع نطاق التبييض الرقمي ليشمل تحويل العائدات غير المشروعة إلى أصول افتراضية، وتجزئة المعاملات عبر منصات الدفع الإلكتروني وإعادة تجميعها عبر شبكات حسابية متشابكة، مما يعقد بشكل جذري عملية تعقب المصدر الأصلي للأموال ويضعف فعالية آليات الكشف التقليدية.

وفي الجانب المؤسسي والأكاديمي، تشير التوجهات الدولية إلى أن الطبيعة العابرة للحدود للعملات الافتراضية تمكن الشبكات الإجرامية من التحايل على الأنظمة الرقابية الوطنية، مما يستلزم تعزيز التعاون العابر للحدود لتبادل المعلومات وتنسيق الإجراءات بشكل آني[1].

[1] Financial Action Task Force, **Virtual assets: Updated guidance for a risk-based approach**, FATF, Paris, 2021, p.12.

وتشير دراسات أكاديمية إلى أن اللامركزية التقنية للعملات المشفرة تضعف القدرة على تحديد هوية المستخدمين، مما يخلق بيئة خصبة للأنشطة غير المشروعة[1]. ويلاحظ أن التطور السريع لتقنيات التعتيم الرقمي، مثل خدمات الخلط والعملات المعززة للخصوصية، يفرض تحديات غير مسبوقة على الجهات الرقابية التي تعتمد على أدوات تحليل تقليدية.

وبناء على هذا التعقيد المتشابك، يتضح أن استيعاب ديناميكيات التبييض الرقمي لم يعد قابلا للاختزال في منظور أحادي أو أداة معزولة، بل يستلزم تبني مقاربة متعددة التخصصات تدمج بدقة بين الكفاءة التقنية المتقدمة لفك تشابك الأنظمة المشفرة، والإلمام القانوني الدقيق لضبط الأطر التشريعية المستجدة، والتحليل السلوكي المعمق لأنماط ارتكاب الجرائم المالية، بما يضمن تصميم منظومات رقابية استباقية وشاملة.

المطلب الثاني: الإطار التنظيمي الدولي والوطني لمكافحة الجرائم المالية الإلكترونية

أصدرت مجموعة العمل المالي (FATF) معايير تنظيمية ملزمة لتنظيم خدمات الأصول الافتراضية، تشترط تطبيق مبدأ السفر، الذي يفرض تبادل بيانات المرسل والمستلم في المعاملات المشفرة التي تتجاوز عتبات مالية محددة، وذلك لضمان إمكانية تتبع التدفقات المالية وكشف الشبكات الإجرامية المستغلة لإخفاء الهوية. كما اعتمدت دول متعددة تشريعات وطنية تلزم مقدمي الخدمات المالية الرقمية بتطبيق إجراءات معرفة العميل بدقة، والإبلاغ الفوري عن المعاملات المشبوهة للسلطات الرقابية المختصة، مما يعزز الشفافية ويسهل التعاون التحقيقي العابر للحدود[2].

[1] Malte Möser & al, an empirical analysis of cryptocurrency laundering, In: **Journal of Financial Crime**, Vol 23, N°3, 2018, p. 895.
[2] Financial Action Task Force, Op.cit, p.12.

غير أن التطبيق الفعلي لهذه المعايير لا يزال يواجه فجوات تشريعية ومؤسسية ملحوظة، خاصة في المناطق التي تفتقر إلى بنية رقابية متكاملة، أو تتعامل مع منصات غير مرخصة تعمل خارج النطاق الجغرافي للولايات القضائية التقليدية. وتشير التقارير الاقتصادية الدولية إلى أن عدم توحيد التعاريف القانونية للأصول الافتراضية، وتباين قدرات الرقابة التقنية بين الدول، يضعف فعالية مبدأ السفر ويخلق فجوات تنظيمية يستغلها الجناة الماليون في عمليات التبييض الرقمي[1].

وتبرز تقارير الأمم المتحدة أن تنسيق الأطر التنظيمية بين الدول يعد شرطا أساسيا لمكافحة الجرائم المالية العابرة للحدود، خاصة في ظل التزايد المطرد لاستخدام المنصات اللامركزية وأدوات تعزيز الخصوصية التي تعقد عمليات التتبع الجنائي. ويؤكد الخبراء أن غياب آليات تبادل المعلومات في الوقت الفعلي، وعدم خضوع بعض مقدمي الخدمات لمعايير الامتثال الموحدة، يولد ثغرات هيكلية تسمح بتدفق الأموال غير المشروعة، عبر شبكات معقدة يصعب فك تشفيرها دون تعاون مؤسسي منسق[2].

وعليه، فإن تطوير الأطر التنظيمية لمكافحة التبييض الرقمي يتطلب مواءمة التشريعات الوطنية مع المعايير الدولية، وتعزيز القدرات التحقيقية الرقمية عبر استثمار أدوات التحليل المتقدم، وإدراج التوعية بالامتثال المالي الرقمي ضمن المناهج المصرفية والتقنية لضمان بناء كوادر مؤهلة قادرة على مواكبة التعقيدات المستجدة.

[1] International Monetary Fund, **Crypto assets and money laundering risks (IMF Working Paper No. 22/45)**, IMF, Washington, 2022, p.18.
[2] United Nations Office on Drugs and Crime, **Cybercrime and digital financial fraud: Global trends and regulatory responses**, UNODC, Vienna, 2022, p.34.

المبحث الثاني: آليات غسل الأموال عبر العملات المشفرة

تمثل العملات المشفرة بيئة خصبة لعمليات التبييض المالي نظراً لطبيعتها اللامركزية، وسرعة انتقالها، وإتاحتها على نطاق عالمي دون حاجة إلى وسيط مصرفي تقليدي. وقد تطورت تقنيات التعتيم الرقمي لتصعب بشكل متزايد عمليات التتبع الرقابي، مما يفرض تحديات غير مسبوقة على الجهات المختصة بمكافحة الجرائم المالية.

المطلب الأول: خصائص العملات المشفرة وسهولة إخفاء الهوية

تعتمد معظم العملات المشفرة على عناوين محفظة رقمية عامة لا ترتبط تلقائيا بالهوية الحقيقية للمستخدم، مما يوفر درجة عالية من الشبه مجهولية تسهل إخفاء هوية الأطراف المشاركة في المعاملات المالية. وتتيح هذه الخاصية التقنية تحويل أصول مالية كبيرة القيمة عبر الحدود الجغرافية خلال ثوان معدودة، ودون المرور عبر القنوات المصرفية التقليدية الخاضعة لأنظمة الرقابة المباشرة ومتطلبات الامتثال المالي المعمول بها دوليا، مما يعزز مرحلة التمويه في دورة غسل الأموال عبر استغلال تعدد المنصات التبادلية وبروتوكولات التحويل لإخفاء المصدر الأصلي للأموال[1].

وتشير تقارير الرقابة الأمنية الأوروبية إلى تصاعد ملحوظ في الاعتماد على الأصول الافتراضية لتمويل الأنشطة غير المشروعة، مع تحول الشبكات الإجرامية نحو منصات لامركزية وأدوات تعزيز الخصوصية لتجاوز متطلبات التحقق من الهوية وتبادل بيانات المعاملات، مما يخلق مساحات تنظيمية يستغلها الجناة الماليون في عمليات التبييض

[1] الاتحاد الدولي للاتصالات، **الأمن السيبراني والوعي الرقمي: اتجاهات عالمية وآليات التطبيق**، منشورات الاتحاد، جنيف، 2022، ص.34.

الرقمي[1]. ويعقد تعدد قنوات التبادل وتنوع البروتوكولات التقنية عملية تحليل التدفقات المالية، مما يفرض على الجهات المختصة تطوير آليات تتبع قادرة على مواكبة التعقيد البنيوي لشبكات البلوك تشين المتشابكة وتجاوز الثغرات التنظيمية بين الولايات القضائية المختلفة.

وتظهر الأدبيات الأكاديمية المحكمة أن نجاعة الأدوات الرقمية في كشف الأنماط الاحتيالية ورصد العمليات المشبوهة ترتبط بعوامل متعددة، منها جودة البيانات المتاحة على الشبكات العامة، وتعقيد الخوارزميات المستخدمة في التحليل السلوكي، وقدرة الأنظمة على التكيف الديناميكي مع تقنيات التعتيم المستجدة[2]. ويؤكد الباحثون أن فعالية التحليل الجنائي الرقمي لا تعتمد فقط على توفر البيانات الخام، بل على قدرة المنهجيات التحليلية على ربط العناوين المشفرة بهويات حقيقية عبر تحليل الشبكات المعقدة، ورصد الأنماط غير الاعتيادية في التحويلات التي تشير إلى عمليات تبييض ممنهجة.

وعليه، فإن تطوير الأطر التنظيمية لمكافحة التبييض عبر العملات المشفرة يتطلب مواءمة التشريعات الوطنية مع المعايير الدولية، وتعزيز القدرات التحقيقية الرقمية عبر استثمار أدوات التحليل المتقدم، وإدراج التوعية بالامتثال المالي الرقمي ضمن المناهج المصرفية والتقنية، مع ضمان خضوع جميع مقدمي خدمات الأصول الافتراضية لنفس معايير الشفافية والمساءلة المالية المعمول بها في القطاع المالي التقليدي.

المطلب الثاني: تقنيات التعتيم الرقمي وسلاسل التبييض المتقدمة

[1] Europol, **Internet organised crime threat assessment (IOCTA) 2023**, European Union Agency for Law Enforcement Cooperation, The Hague, 2023, p.47.
[2] Rainer Böhme & al, Bitcoin: Economics, technology, and governance, In: **Journal of Economic Perspectives**, Vol 29, N°2, 2015, p.225.

تشكل تقنيات التعتيم الرقمي، كخدمات الخلط والعملات المعززة للخصوصية ومنصات التبادل اللامركزية، أدوات جوهرية تستغل لفك الارتباط بين العناوين المشفرة وسجلات المعاملات الأصلية، مما يعقد عمليات التتبع الجنائي التقليدي ويطيل زمن الاستجابة المؤسسية، لا سيما مع شيوع أسلوب القفز بين السلاسل الذي يقلل دقة الأدوات الرقابية عبر تنقل الأصول بين شبكات متباينة البروتوكولات[1].

وفي الجانب التشريعي، تصنف التوجيهات المعتمدة من مجموعة العمل المالي تنظيم مقدمي خدمات الخلط والبروتوكولات المعززة للخصوصية كأولوية رقابية عاجلة، نظرا لقدرتها الهيكلية على التحايل على متطلبات مبدأ السفر ومعايير التحقق من الهوية، مما يستلزم مواءمة فورية للأطر الوطنية مع المعايير الرقابية الدولية لضمان عدم تحول هذه المنصات إلى مساحات تنظيمية غير خاضعة للمساءلة[2].

كما يساهم التطور المتسارع في خوارزميات الذكاء الاصطناعي في تمكين الشبكات الإجرامية من تصميم نماذج تمويه ديناميكية تتكيف آليا مع أنظمة الرصد، مما يفرض على الجهات المشرفة تبني منظومات تحليلية هجينة تدمج أدوات تحليل سلاسل الكتل المتقدمة مع نماذج التعلم الآلي للكشف عن الأنماط السلوكية الشاذة ورصد التدفقات غير المشروعة قبل اندماجها في الاقتصاد الرسمي[3].

وعليه، فإن التصدي الفعال لهذه الظاهرة يستلزم استثمارا مؤسسيا مستداما في البحث والتطوير الرقابي، وتعزيز الشراكات الاستراتيجية بين البنوك المركزية ومزودي خدمات البلوك تشين وشركات الأمن السيبراني، بالإضافة إلى اعتماد أطر تنظيمية مرنة

[1] Europol, **Op.cit**., p.52.
[2] Financial Action Task Force, **Op.cit**., p.24.
[3] Chainalysis, **The 2024 crypto crime report**, Chainalysis Inc, New York, 2024, p.31.

قابلة للتطوير المستمر، بما يضمن مواكبة الابتكارات التقنية المتسارعة دون تعطيل مسار الابتكار المالي المشروع أو تقويض الشفافية الرقابية.

المبحث الثالث: استغلال بطاقات الدفع الإلكتروني في العمليات المالية غير المشروعة

رغم أن بطاقات الدفع الإلكتروني تخضع لإشراف مصرفي مباشر، إلا أن ثغرات الأنظمة الإلكترونية، وسرعة انتشار المحافظ الرقمية، وتعدد قنوات الدفع، تخلق مسارات غير مرئية تستغل في تبييض العائدات غير المشروعة، خاصة عبر شبكات الحسابات الوهمية والتحويلات المجزأة.

المطلب الأول: ثغرات الأنظمة البنكية الإلكترونية والاحتيال المرتبط بالبطاقات

على الرغم من إخضاع بطاقات الدفع الإلكتروني لأنظمة رقابة مصرفية مؤسسية، إلا أن تعقيد البنى التحتية الرقمية وتباين معايير الأمن السيبراني بين المؤسسات المالية يخلقان فجوات استغلالية متزايدة، تستغل فيها ثغرات التوثيق الضعيف لا سيما في المعاملات عن بعد عبر استخدام بيانات مسروقة أو مولدة آليا، مما يستدعي توحيد بروتوكولات التحقق عبر الحدود لضمان عدم التحايل على الضوابط الأساسية قبل تفعيل أنظمة الرصد[1].

ويتطلب التصدي لهذه القنوات غير المشروعة معالجة استغلال أجهزة نقاط البيع المخترقة، وشبكات الوسطاء الماليين الوهميين التي تعيد توجيه العائدات عبر سلاسل تحويل متعاقبة لتعقيد المسار الرقابي، مما يفرض اعتماد معايير امتثال موحدة تلزم

[1] Bank for International Settlements, **Annual economic report 2023: Payment systems and financial stability**, BIS, Basel, 2023, p.14.

جميع مقدمي خدمات الدفع بنفس متطلبات الإفصاح والمساءلة بغض النظر عن حجمهم أو طبيعة تراخيصهم[1].

كما تؤكد التقارير المؤسسية أن تأخر تحديث خوارزميات كشف الشذوذ السلوكي، بالتزامن مع التوسع السريع في المحافظ الرقمية والتطبيقات المالية الناشئة، يولد قنوات موازية للاستغلال عندما تفلت هذه المنصات من الأطر الرقابية التقليدية، مما يضعف القدرة على رصد التدفقات المشبوهة في الوقت الفعلي، ويستدعي مواءمة التشريعات الوطنية مع المعايير الدولية لحماية المستهلك الرقمي[2].

وعليه، فإن سد هذه الثغرات الهيكلية يستلزم إعادة هندسة نماذج المراقبة المصرفية لتعتمد على التحليل التنبئي القائم على الذكاء الاصطناعي، ورفع كفاءة البروتوكولات التشفيرية، وتعزيز آليات التبادل الفوري لمؤشرات التهديد بين البنوك والجهات الرقابية، بما يحول منظومة الكشف من رد فعل تأخيري إلى وقاية استباقية قادرة على مواكبة ديناميكيات الاحتيال المالي المعاصر.

المطلب الثاني: شبكات التبييض عبر المحافظ الإلكترونية والتحويلات المتعددة

يشهد الاحتيال المالي المعاصر تحولا متسارعا نحو استغلال المحافظ الإلكترونية وأنظمة الدفع البديل، نظرا لمرونتها التشغيلية وقدرتها على تنفيذ التحويلات العابرة للحدود دون المرور بالقنوات المصرفية التقليدية، مما يتيح للمجرمين اعتماد أسلوب

[1] صندوق النقد العربي، **التحول الرقمي وحماية المستهلك المالي في المنطقة العربية**، إدارة الدراسات والبحوث، أبو ظبي، 2022، ص.52.

[2] United Nations Office on Drugs and Crime, Op.cit., p.41.

التجزئة الهيكلي لتقسيم المبالغ الكبيرة إلى تحويلات صغيرة ومتكررة، تتجاوز عتبات الإبلاغ الإلزامي وتخترق الضوابط الرقابية الوطنية[1].

ويتطلب التصدي لهذه الثغرات معالجة استغلال البطاقات المدفوعة مسبقا غير المرتبطة بهويات حقيقية، والفجوات التنظيمية الناتجة عن غموض الحدود بين مقدمي الخدمات المالية التقليدية وشركات التقنية المالية الناشئة، حيث تتيح هذه المنصات قنوات موازية لدمج العائدات غير المشروعة تدريجيا في الدورة الاقتصادية الرسمية عبر قطاعات التجارة الإلكترونية والألعاب الرقمية دون خضوع لمتطلبات الإفصاح الموحدة[2].

كما تبرز الدراسات المتخصصة أن نجاعة المواجهة الحديثة لهذه الشبكات رهينة بقدرة الأجهزة الرقابية على تحليل شبكات العلاقات المعقدة بين الحسابات الرقمية، حيث يحسن دمج تقنيات تحليل الرسوم البيانية مع خوارزميات التعلم الآلي بشكل ملحوظ قدرة الأنظمة على كشف الحلقات المالية المغلقة، وإعادة توجيه التدفقات المشبوهة قبل استقرارها في الاقتصاد النظامي، متجاوزة بذلك حدود الرصد التقليدي المعتمد على القواعد الثابتة[3].

وبالتالي، فإن مواجهة هذه الشبكات المعقدة تستلزم تبني منصات مراقبة مركزية تعتمد على التحليل التنبئي والشبكي، وتعزيز الشراكات المؤسسية العابرة للحدود لتبادل مؤشرات التهديد في الوقت الفعلي، وضمان خضوع جميع قنوات الدفع الرقمي لمعايير شفافية ومساءلة موحدة، بما في ذلك غير النمطية.

[1] Financial Action Task Force, Op.cit., p.28.
[2] United Nations Office on Drugs and Crime, Op.cit., p.45.
[3] Chainalysis, Op.cit., p.38.

الخاتمة:

خلصت هذه الدراسة إلى أن التبييض الرقمي تجاوز كونه ظاهرة عابرة ليشكل منظومة إجرامية هيكلية مترابطة، توظف التشابك التقني، والانسيابية الفائقة في المعاملات الإلكترونية، والتفاوت التشريعي بين الدول. وأظهر التحليل أن الأصول الافتراضية تتيح حجب البصمة الرقمية عبر بروتوكولات التشفير المتقدم والبنى اللامركزية، في حين يستغل ضعف آليات التحقق في معاملات البطاقات الإلكترونية والثغرات النظامية لتفتيت التدفقات المالية، وإعادة توجيهها عبر مسارات متشعبة.

وكشفت المراجعة الرقابية أن المنظومات الإشرافية الراهنة، رغم مسارات تطويرها، لا تزال تواجه قصورا في الرصد اللحظي، والتدفق المعلوماتي العابر للحدود، واستيعاب التسارع التقني. وعليه، فإن التصدي الفعال لهذه الظاهرة يستلزم نهجا متكاملا يوائم بين التطوير التشريعي، والرقمنة المؤسسية، والشراكات الاستراتيجية المستدامة.

وانطلاقا مما سبق، تقدم الدراسة مجموعة من التوجهات العملية، أهمها:

- تبني أنظمة كشف قائمة على الذكاء الاصطناعي، وتحليل سلاسل الكتل لرصد الأنماط غير الاعتيادية في المعاملات المشفرة والإلكترونية بشكل فوري.
- إلزام جميع مقدمي خدمات الأصول الافتراضية ومنصات الدفع الإلكتروني بتبادل بيانات المرسل والمستلم تلقائيا، بما يتوافق مع معايير مجموعة العمل المالي.
- تصنيف خدمات الخلط الرقمي والعملات المعززة للخصوصية ضمن الكيانات الخاضعة للترخيص والرقابة المالية، مع فرض شفافية في بروتوكولات المعالجة.
- إنشاء منصات مشتركة بين البنوك المركزية، وشركات التقنية المالية، والجهات الرقابية لتبادل مؤشرات التهديد وتحديث نماذج الكشف بشكل دوري.

- مواءمة التشريعات المحلية مع المعايير الدولية، وتعزيز القدرات التحقيقية الرقمية، وإدراج التوعية بالامتثال المالي الرقمي ضمن المناهج المصرفية والتقنية.

قائمة المراجع:

1-مقال في المجلات:

- Böhme Rainer & al, Bitcoin: Economics, technology, and governance, In: **Journal of Economic Perspectives**, Vol 29, N°2, 2015.
- Möser Malte & al, an empirical analysis of cryptocurrency laundering, In: **Journal of Financial Crime**, Vol 23, N°3, 2018.

2-**التقارير** :

- الاتحاد الدولي للاتصالات، **الأمن السيبراني والوعي الرقمي: اتجاهات عالمية وآليات التطبيق**، منشورات الاتحاد، جنيف، 2022.
- صندوق النقد العربي، **التحول الرقمي وحماية المستهلك المالي في المنطقة العربية**، إدارة الدراسات والبحوث، أبو ظبي.
- Bank for International Settlements, **Annual economic report 2023: Payment systems and financial stability**, BIS, Basel, 2023.
- Chainalysis, **The 2024 crypto crime report**, Chainalysis Inc, New York, 2024.
- Europol, **Internet organised crime threat assessment (IOCTA) 2023**, European Union Agency for Law Enforcement Cooperation, The Hague, 2023.
- Financial Action Task Force, **Virtual assets: Updated guidance for a risk-based approach**, FATF, Paris, 2021.
- International Monetary Fund, **Crypto assets and money laundering risks (IMF Working Paper No. 22/45)**, IMF, Washington, 2022.

- United Nations Office on Drugs and Crime, **Cybercrime and digital financial fraud: Global trends and regulatory responses**, UNODC, Vienna, 2022.