



الآليات القانونية والأمنية لمكافحة الجريمة السيبرانية

وغسل الأموال الإلكتروني

أكرم صالح محمد عرب

طالب باحث بسلك الدكتوراه

تخصص القانون الخاص

جامعة محمد الخامس – الرباط

تحت إشراف دة. لطيفة المهداتي أستاذة التعليم العالي
المغرب

الملخص:

يستعرض البحث ظاهرة تفاقم الجرائم السيبرانية واقتراحها الجسيم بعمليات غسل الأموال الإلكترونية عبر التطور المتسارع للمنصات الرقمية والعمليات المشفرة، ويسلط الضوء على خطورة هذه الجرائم على استقرار النظام المالي العالمي وأمن المجتمعات. وتدور الإشكالية حول تقييم مدى كفاية وجاهزية المنظومات القانونية والأمنية (على المستويين الوطني والدولي) للحد من الجرائم السيبرانية ومواجهة الأساليب المتطورة لتدوير الأموال غير المشروعة عبر الفضاء الرقمي. ولقد تم اعتماد المنهج الوصفي التحليلي لتفكيك مفاهيم الجريمة الرقمية وغسل الأموال واستعراض الأطر التشريعية، بالاستعانة بالمنهج المقارن لبيان كفاءة الآليات الأمنية والتقنية والتحديات الميدانية التي تواجه سلطات إنفاذ القانون في مختلف المنظومات. وأخيرا توصل البحث إلى أن الثغرات الإجرائية وتشتت التعاون الدولي يُضعفان جهود مكافحة، وخلص إلى أهمية تبني آليات الرصد التقني الاستباقي وتطوير أدلة إثبات جنائية رقمية معتمدة، مع ضرورة تحديث القوانين الوطنية لتواكب مستجدات العملات المشفرة والذكاء الاصطناعي.

الكلمات المفتاحية: الآليات القانونية والأمنية – الجريمة السيبرانية – غسل الأموال.



المقدمة:

تعدّ الجريمة السيبرانية وغسل الأموال الإلكتروني من أخطر التحديات الناشئة التي تواجه الدول في العصر الرقمي الحديث، فقد أدّى التطور الهائل في تقنيات الاتصالات والمعلومات، وانتشار الشبكات المالية الرقمية والعملات المشفرة، إلى خلق بيئة خصبة لعصابات الجريمة المنظمة العابرة للحدود لتنفيذ أنشطتها الإجرامية بعيداً عن الرقابة التقليدية.

وتتميز الأنشطة الإجرامية السيبرانية بطبيعتها المعقدة وتخفي مرتكبيها خلف هوامش الخصوصية الرقمية والتشفير، وتكمن خطورتها في قدرة الجناة على إعادة تدوير الأموال المتحصلة من جراء هذه الممارسات الإجرامية واختلاس البيانات وحجب الخدمة، وتميرها عبر منصات المعاملات المالية الإلكترونية والمؤسسات المصرفية الرقمية بغرض تعمية مصدرها غير المشروع.

وأمام هذا المشهد المتغير، باتت المنظومات التشريعية الوطنية والقوانين الجنائية القائمة عاجزة بمفردها عن ملاحقة الفاعلين واقتفاء أثر الأصول الرقمية المهربة، وهو ما فرض على المشرّعين ضرورة تحديث قواعد الإثبات الجنائي، وابتكار نصوص قانونية تُجرّم الأفعال الناشئة في الفضاء الإلكتروني، واستحداث أطر جديدة للتعاون القضائي الدولي.

وفي السياق ذاته، لم يعد البعد القانوني وحده كافياً، بل فرض هذا الواقع تطوير آليات أمنية وتقنية متقدمة، وشمل ذلك تأسيس فرق الاستجابة للطوارئ السيبرانية، وتدريب الوحدات المختصة في التحقيق الرقمي، وتطوير أدوات أدلة إثبات جنائية رقمية (Digital Forensics) تكون قادرة على تتبع الأثر الرقمي وضبط الأصول المشفرة.

وتتضح أهمية دراسة الآليات القانونية والأمنية لمكافحة الجريمة السيبرانية وغسل الأموال الإلكتروني في كشف طبيعة التكامل والتناسق بين القاعدة القانونية والتدبير الأمني، بهدف حماية الاقتصاد الوطني، وضمان استقرار المرفق المالي، وصون الأمن القومي للدول من المخاطر الرقمية المتزايدة.

وتكمن الفكرة المحورية للإشكالية في التزاغ القائم بين سرعة تطور تقنيات الأجرام الرقمي وأساليب إخفاء الأموال غير المشروعة عبر الفضاء السيبراني من جهة، ومدى كفاءة وملاءمة الأطر التشريعية والآليات الأمنية الوطنية والدولية المستحدثة لتطبيق هذا الإجراء من جهة أخرى.

إلى أي مدى تُساهم الآليات القانونية والأمنية المستحدثة في مواجهة الجريمة السيبرانية وحدّ نجاعة عمليات غسل الأموال الإلكترونية في ظل الرهانات التقنية والعابرة للحدود؟

ويتفرع عن الإشكالية المركزية مجموعة من الأسئلة من قبيل:

- (1) ما هو الإطار المفهومي والجنائي للجريمة السيبرانية وعلاقتها بغسل الأموال الإلكتروني؟
 - (2) ما هي الآليات القانونية والإجرائية الوطنية والدولية للحد من الأنشطة المالية الإلكترونية المشبوهة؟
 - (3) كيف تساهم المنظومات والآليات الأمنية والتقنية في تتبع الجرائم الإلكترونية ورصد الأموال المهربة؟
 - (4) ما هي أبرز التحديات والإكراهات الميدانية التي تواجه مكافحة الإجرام السيبراني وغسل الأموال الرقمي؟
- للإجابة عن الإشكالية المركزية والأسئلة المتفرعة عنها أقترح الخطاطة الآتية:

– المحور الأول: الإطار القانوني والمفهومي لمكافحة الجريمة السيبرانية وغسل الأموال الإلكتروني

– المحور الثاني: الآليات الأمنية والتحديات العملية في مواجهة غسل الأموال الإلكتروني



المحور الأول: الإطار القانوني والمفاهيمي لمكافحة الجريمة السيبرانية وغسل الأموال الإلكتروني

شهد العالم مع مطلع القرن الحادي والعشرين تحولاً بنيرياً واسع النطاق نحو اعتماد البيئات الرقمية والشبكات المعلوماتية في مجمل النشاطات الإنسانية والمالية، وقد أفرز هذا التحول الرقمي المتسارع نمطاً إجرامياً حديثاً يتجاوز الحدود الجغرافية التقليدية، حيث أصبحت البيئة السيبرانية مسرحاً لارتكاب جرائم معقدة تستهدف البيانات والأنظمة والمؤسسات على حد سواء.

وتُعدّ الجريمة السيبرانية المدخل الرئيس لتوليد عائدات مالية ضخمة غير مشروعة، مما فرض ظاهرة تدوير وتبيض هذه الأموال عبر وسائط رقمية معقدة، واقتراح الجرائم الإلكترونية بعمليات غسل الأموال الرقمية شكّل حلقة إجرامية مفرغة تعتمد على سرعة المعاملات وسرية المتداولين، وهو ما فرض على التشريعات الجنائية إعادة النظر في قواعد التجريم والإثبات التقليدية لمواجهة هذه المخاطر.

وأمام هذه التحولات، غدت الحاجة ملحة لصياغة أطر مفهومية دقيقة وتطوير قواعد قانونية وإجرائية وطنية ودولية تكون قادرة على ملاحقة الفاعلين وتحميد أصولهم الرقمية. وعلى هذا الأساس، يتم تناول هذا المحور من خلال مطلبين رئيسين: يُخصص المطلب الأول لبحث "الإطار المفاهيمي والجنائي للجريمة السيبرانية وعلاقتها بغسل الأموال الإلكتروني"، بينما يركز المطلب الثاني على دراسة "الآليات القانونية والإجرائية الوطنية والدولية للحد من الأنشطة المالية الإلكترونية المشبوهة".

المطلب الأول: الإطار المفاهيمي والجنائي للجريمة السيبرانية وعلاقتها بغسل الأموال الإلكتروني

تُشكل الجريمة السيبرانية مظلة واسعة لصور شتى من الأفعال غير المشروعة التي تتم باستخدام الموارد الحاسوبية والشبكات الرقمية، ويعود التحديد المفاهيمي لهذه الجرائم إلى طبيعتها المعقدة وتطوير وسائلها باستمرار، مما جعلها تبتعد عن المفاهيم التقليدية للجريمة الجنائية من حيث أسلوب التنفيذ ونوعية الأدلة ومحيط السلوك الإجرامي.

ولم تُعدّ الجريمة السيبرانية تقتصر على مجرد التعطيل الفني أو الاختراق المحض، بل تحولت إلى صناعة مادية تُدر أرباحاً هائلة على عصابات الإجرام المنظم، وهنا تبرز علاقتها العضوية بغسل الأموال الإلكتروني، إذ تحاول الشبكات الإجرامية تدوير هذه العائدات غير المشروعة باستغلال غياب الحدود الرقمية وسرعة تدفق الأموال عبر الإنترنت.

وقد استغل غاسلو الأموال الإلكتروني الثورة التكنولوجية وما رافقها من ظهور للعمليات المشفرة والمنصات المفتوحة لإعادة ضخ تلك الأموال في العروق الاقتصادية الشرعية، وتعتمد هذه الأساليب الحديثة على التمويه والتجزئة والتشفير، وهو ما يُضاعف صعوبة التعرف على المصدر الإجرامي الحقيقي لتلك التدفقات المالية.

وللتعمق في التوصيف الجنائي والفني لهذه الظاهرة المتطورة، يتوزع هذا المطلب على فرعين أساسيين: يُعالج في أولاً موضوع "ماهية الجريمة السيبرانية وآليات غسل الأموال الإلكتروني عبر المنصات الرقمية"، في حين يُخصص ثانياً لتفصيل "صور وأساليب تدوير الأموال غير المشروعة باستعمال التقنيات الحديثة والعملات المشفرة".

أولاً: ماهية الجريمة السيبرانية وآليات غسل الأموال الإلكتروني عبر المنصات الرقمية.

تُعرّف الجريمة السيبرانية بأنها كل سلوك غير مشروع يُرتكب باستعمال شبكات المعلومات، أو الحاسب الآلي، أو الوسائل الإلكترونية المتقدمة، ويهدف إلى الاعتداء على البيانات أو الأجهزة أو الأنظمة الرقمية، أو استغلالها لإلحاق الضرر بالأفراد والمؤسسات، وتتميز هذه الجرائم بطبيعتها اللاإقليمية وخلوها من الحدود الجغرافية التقليدية، مما يجعلها تشكل نمطاً إجرامياً عابراً للحدود الوطنية بسرعة فائقة



وحجم أضرار عالي التعقيد¹. وتعتمد هذه الجرائم على توظيف البيئة البرمجية المعقدة وتقنيات التشفير العالية، مما يمنح الفاعلين قدرة هائلة على التخفي وعدم ترك آثار مادية ملموسة تُسهل الوصول إلى هوياتهم الحقيقية².

وترتبط الجريمة السيبرانية بعمليات غسل الأموال الإلكتروني بعلاقة سببية عضوية؛ حيث تُعدّ الجرائم الإلكترونية (كالحجمات الفدية، واختراق الحسابات البنكية، والتزوير الإلكتروني، والاحتيال المالي عبر الإنترنت) مصدراً رئيساً لتوليد الأموال القذرة وغير المشروعة التي تحتاج إلى التدوير والتبييض، وتتجسد عملية غسل الأموال الإلكتروني في نقل وتدوير هذه العائدات الإجرامية عبر المنصات الرقمية ووسائل الدفع الحديثة لإخفاء مصدرها الأصلي وتزوير مشروعيته³، ويستفيد غاسلو الأموال في هذا الصدد من السرعة الهائلة للمعاملات المالية عبر شبكة الإنترنت التي تتم دون الحاجة للحضور الفعلي للعميل، مما يُضعف وسائل الرقابة التقليدية⁴.

وتعتمد آليات غسل الأموال عبر المنصات الرقمية على استخدام المحافظ الإلكترونية المتعددة والخدمات البنكية عبر الإنترنت، حيث يتم تقسيم المبالغ الضخمة إلى معاملات مالية صغيرة جداً وتوزيعها على مئات الحسابات الوهمية فيما يعرف باستراتيجية "التفتيت" أو (Smurfing)، وتتيح هذه التقنية تجاوز المعايير الرقمية للتنبيه الآلي الخاصة بنظم الامتثال في البنوك، إذ تمر المعاملات القليلة القيمة دون إثارة الشكوك الإدارية أو الأمنية⁵، كما تُستغل منصات تجارة الألعاب الإلكترونية والتطبيقات التفاعلية في شراء وبيع الأصول الافتراضية داخل الألعاب، ثم إعادة تحويلها إلى أموال نقدية حقيقية عبر منصات الوساطة المالية الخارجية⁶.

إلى جانب ذلك، تُشكّل مؤسسات الصرافة الافتراضية والشركات المالية الرقمية غير الخاضعة للتنظيم حلقة وصل رئيسة في دورة غسل الأموال الإلكتروني. إذ توفر هذه الكيانات الفرصة لتحويل العائدات غير المشروعة بين بطاقات الائتمان مسبقة الدفع والتطبيقات المالية دون تطبيق صارم لإجراءات "اعرف عميلك" (KYC)⁷، وبسبب هذا التعقيد الهيكلي والتكنولوجي، أصبحت المنصات الرقمية تشكل بيئة جاذبة لعصابات الجريمة المنظمة، التي باتت تعتمد على الحلول التقنية لتبييض أرباحها وتجنب أي ملاحقة أمنية أو مصادرة قضائية للأصول⁸.

ثانياً: صور وأساليب تدوير الأموال غير المشروعة باستعمال التقنيات الحديثة والعملات المشفرة.

تعد العملات المشفرة، وفي مقدمتها البتكوين (Bitcoin) والعملات ذات الخصوصية العالية كـ (Monero) و (Zcash)، المعبر الأساسي لعمليات غسل الأموال الإلكتروني في العصر الحديث، وتعتمد هذه العملات على تقنيات التشفير اللامركزي وتكنولوجيا البلوكتشين (Blockchain)، والتي تضمن سرية هوية المتداولين واستبدال أسمائهم بعناوين رقمية مشفرة تتكون من سلسلة من الحروف

¹ - أبو الفتوح، عبد الفتاح. المسؤولية الجنائية عن الجرائم السيبرانية وآليات مكافحتها: دراسة مقارنة. دار النهضة العربية، القاهرة. (2021).

² - سليمان، أحمد فاروق. غسل الأموال عبر الوسائط الإلكترونية والعملات الرقمية المشفرة. دار الفكر الجامعي، الإسكندرية. (2020).

³ - المالكي، محمد الأمين. التحقيق الجنائي الرقمي والدليل الإلكتروني في المواد الجنائية. مجلة العلوم القانونية والأمنية، المجلد 5، العدد 2، (2022). ص ص 45-78.

⁴ - Brenner, S. W. Cybercrime: Criminal Threats to the Digital Age. ABC-CLIO / Praeger, Santa Barbara. (2010).

⁵ - أبو الفتوح، عبد الفتاح. م.س

⁶ - Brenner, S. W. op.cit

⁷ - سليمان، أحمد فاروق. م س

⁸ - المالكي، محمد الأمين. م س



والأرقام⁹، وهذا الاختفاء خلف عناوين التشفير يجعل التتبع المباشر لمالك الحساب الحقيقي أمراً بالغ الصعوبة بالنسبة للسلطات الرقابية والأمنية، ويمنح الجناة غطاءً آظناً لتحويل المبالغ الطائلة بين مختلف دول العالم في ثوانٍ معدودة¹⁰.

ولزيادة تعقيد التتبع المالي، تلجأ العصابات الإجرامية إلى استخدام أساليب تقنية متطورة تُعرف بـ "الخلاطات" أو "المزاج الرقمية" (Crypto Mixers / Tumblers)، وتقوم هذه الخدمات باستلام العملات المشفرة من عدة مصادر مختلفة ودمجها وتجزئتها في خوارزميات معقدة، ثم إعادة إرسالها إلى عناوين مخرجات جديدة ومختلفة بنسب تتطابق مع القيمة الأصلية بعد اقتطاع عمولة الخدمة¹¹، وتؤدي هذه العملية إلى قطع الصلة المباشرة بين العنوان المصدر للعملة الملوثة والعنوان المستلم النهائي، مما يقضي على المسار التحليلي لتقنية البلوكشين ويُحيل عملية تتبع السلسلة إلى طريق مسدود¹².

كما ظهرت آلية تدوير حديثة عابرة للشبكات تُعرف بـ "التحويل بين سلاسل الكتل" أو (Chain-Hopping)، والتي تتضمن التحويل المتعدد والمفاجئ للعملات من نوع مشفر إلى نوع آخر عبر منصات التداول اللامركزية (DEXs) التي لا تطلب إثباتات الهوية شخصية¹³، ويقوم الجاني مثلاً بتحويل أرباح هجمات الفدية المأخوذة بالبتكوين إلى عملة مكسورة التتبع كـ (Monero)، ثم تحويلها مجدداً إلى عملات استقرار (Stablecoins) كـ (USDT)، مما يجعل اقتفاء الأثر عبر منصات الاستكشاف المتعددة مستحيلاً تقريباً على التحريات التقليدية¹⁴.

وأخيراً، يتم دمج هذه الأصول المشفرة في الاقتصاد الرسمي عبر تحويلها إلى أصول نقدية حقيقية (Fiat Money) باستخدام منصات التداول من شخص لشخص (P2P) أو عبر شبكات أجهزة الصراف الآلي الخاصة بالعملات المشفرة (Crypto ATMs) التي ينتشر بعضها في دول تفتقر لرقابة تنظيمية صارمة¹⁵، فضلاً عن ذلك، ظهر اتجاه حديث لاستغلال الرموز غير القابلة للاستبدال (NFTs) والعقارات الافتراضية في عوالم (Metaverse)، حيث يتم تضخيم أسعار هذه الأصول الرقمية اصطناعياً وشرائها بأموال غير مشروعة لإضفاء صفة "الأرباح الاستثمارية" عليها في نهاية الدورة الإجرامية¹⁶.

المطلب الثاني: الآليات القانونية والإجرائية الوطنية والدولية للحد من الأنشطة المالية الإلكترونية المشبوهة

استوجب التهديد المتزايد للجرائم السيبرانية والمالية تحركاً تشريعياً لمواجهة الفراغ القانوني الذي أحدثته التطور التكنولوجي، فكان على التشريعات الوطنية سحب أحكام القانون الجنائي وقواعد الإجراءات الجنائية التقليدية وتعديلها أو إصدار قوانين خاصة لضمان إضفاء صفة المشروعية على تتبع الأنشطة المالية الرقمية وملاحقتها.

⁹ – King, R., & Walker, C. (2019). Money Laundering in the Digital Era: Cryptocurrencies and Cybercrime Exploitation. Routledge, London.

¹⁰ – United Nations Office on Drugs and Crime (UNODC). (2021). Comprehensive Study on Cybercrime and Electronic Financial Crimes. UN Publishing, Vienna.

¹¹ – King, R., & Walker, C. op.cit.

¹² – Dupuis, N., & Smith, M. (2022). Cryptocurrency Laundering Mechanics and Anonymity Networks. Journal of Financial Crime, 29(3), 882–899.

¹³ – United Nations Office on Drugs and Crime (UNODC). Op.cit .

¹⁴ – Choo, K. K. R. (2023). Advanced Digital Forensics and Financial Cybercrime Investigation. Springer International Publishing, Cham.

¹⁵ – Dupuis, N., & Smith, M. op.cit.

¹⁶ – Choo, K. K. R. op.cit.



وعلى مستوى القوانين الداخلية، سعت الدول إلى سن قواعد إجرائية مرنة تتيح لضباط العدلية وسلطات التحقيق التعامل مع الأدلة المعنوية والرقمية، بدءاً من الحفظ العاجل للبيانات وصولاً إلى أوامر التفتيش والضبط للأنظمة والحسابات المصرفية الإلكترونية، مع إرساء الالتزامات القانونية على عاتق المؤسسات المالية للحظر والإبلاغ عن أي حركة مشبوهة.

إلا أن النطاق الوطني يظل محدوداً الفاعلية نظراً للطبيعة العابرة للحدود التي تتميز بها الشبكات المعلوماتية؛ إذ إن السلوك الإجرامي قد يتم في دولة والنتيجة تظهر في دولة أخرى والأموال تُهرَّب إلى دولة ثالثة، ومن هذا المنطلق ظهرت الحاجة الماسة لإنشاء قواعد اتفاقية دولية وإطارات ملزمة للتعاون والإنابات القضائية لتسليم المجرمين وتجميد الأصول.

ولسبر أغوار هذين البعدين الوطني والدولي ومدى تكاملهما في الرادع القانوني، يُعالج هذا المطلب عبر قسمين متتابعين: حيث يدرس أولاً موضوع "قواعد التحريم والقوانين الإجرائية الوطنية الخاصة بالجرائم الإلكترونية والمالية"، وينتقل في ثانياً لبحث "الاتفاقيات الدولية وأطر التعاون القضائي والإنابات القضائية العابرة للحدود

أولاً: قواعد التحريم والقوانين الإجرائية الوطنية الخاصة بالجرائم الإلكترونية والمالية.

اتجهت التشريعات الوطنية الحديثة نحو إعادة صياغة قواعد التكيف والجريمة لملائمة الطبيعة الرقمية للجرائم المعاصرة، حيث تم سن قوانين خاصة بمكافحة الجرائم المعلوماتية تضمنت نصوصاً صريحة تُجرّم الاختراق، والدخول غير المشروع، وتدمير البيانات، والتزوير الإلكتروني¹⁷، وقد افترض المشرع الجنائي قواعد التحريم هذه لحماية سلامة الفضاء الرقمي، مع ربطها بقوانين مكافحة غسل الأموال الوطنية التي جرى تعديلها لكي تشمل الأصول الافتراضية والمعاملات الرقمية ضمن نطاق الأموال الخاضعة لأحكام التحريم والمصادرة¹⁸.

وعلى الصعيد الإجرائي الجنائي، فرض التطور التكنولوجي التخلي عن قواعد التفتيش والضبط التقليدية وصياغة أحكام إجرائية رقمية تتيح للضابطة العدلية وسلطات التحقيق التعامل مع "الدليل الرقمي"، واشتملت هذه القوانين على صلاحية إصدار أمر بالأمر بالحفظ العاجل للبيانات المخزنة لدى مزودي خدمات الإنترنت، وأوامر الاعتراض والتنصت المباشر على حركة البيانات المالية المشبوهة بإذن قضائي مسبق¹⁹، كما أطرّت القوانين الوطنية القواعد الخاصة بقبول الدليل الرقمي أمام المحاكم الشرعية والجنائية بشرط سلامة السلسلة الحسابية للبيانات وتطبيق معايير الموثوقية الجنائية²⁰.

بالإضافة إلى التحري الإجرائي، فرضت القوانين الوطنية التزامات مشددة على الكيانات المالية والمصرفية ومزودي خدمات الأصول الافتراضية (VASPs)، وألزمتهما النصوص القانونية بتطبيق إجراءات العناية الواجبة تجاه العملاء، وإجراءات التعرف على المستفيد الحقيقي، والالتزام الفوري بالإبلاغ عن المعاملات المالية المشبوهة إلى وحدات التحريات المالية (FIU) عند تجاوز المعاملات سقفاً مالياً محددًا أو اتسامها بنمط معقد وغير مبرر استثمارياً²¹.

غير أن تطبيق هذه القواعد الوطنية يتصادم باستمرار مع صعوبات إجرائية جسيمة، في مقدمتها التنازع في الاختصاص القضائي بسبب ارتكاب السلوك الإجرامي في دولة وتحقيق النتيجة في دولة أخرى واستفادة المكتسبات في دولة ثالثة²²، كما تظهر عقبة إثبات "العلم

17 - أبو الفتوح، عبد الفتاح. المسؤولية الجنائية عن الجرائم السيبرانية وآليات مكافحتها: دراسة مقارنة. دار النهضة العربية، القاهرة. (2021).

18 - سليمان، أحمد فاروق. م.س.

19 - عبد الله، خالد مصطفى. (2019). الإثبات الجنائي في الجرائم الإلكترونية: دراسة مقارنة حول قبول الدليل الرقمي. منشورات الحلبي الحقوقية، بيروت.

20 - المالكي، محمد الأمين. م.س.

21 - سليمان، أحمد فاروق. م.س.

22 - عبد الله، خالد مصطفى. (2019). الإثبات الجنائي في الجرائم الإلكترونية: دراسة مقارنة حول قبول الدليل الرقمي. منشورات الحلبي الحقوقية، بيروت.



والنية الإجرامية" لدى المتداولين في منصات التشفير، مما دفع التشريعات إلى التوسع في الاعتماد على قرائن القرائن المالية والتفتيش الاستباقي للأصول للحيلولة دون تهريب العائدات الرقمية قبل صدور الأحكام القضائية النهائية²³.

ثانياً: الاتفاقيات الدولية وأطر التعاون القضائي والإنابات القضائية العابرة للحدود.

نظراً للطبيعة العابرة للحدود التي تتميز بها الجريمة السيبرانية وغسل الأموال الرقمي، أصبح التعاون الدولي حجر الزاوية في المنظومة القانونية لمكافحة، وتُعد اتفاقية بودابست لمكافحة الجرائم السيبرانية (2001) البروتوكولات الملحق بها الصك القانوني الدولي الأول والأكثر شمولاً؛ إذ وضعت الإطار الإجرائي للتعاون الدولي السريع، والتفتيش العابر للحدود، وتبادل الأدلة الرقمية بين الدول الأطراف، فضلاً عن إنشاء شبكة 7/24 للاتصال السريع لملاحقة الجرائم السيبرانية وتجميد البيانات الرقمية فوراً²⁴.

وعلى المستوى المالي، تلعب مجموعة العمل المالي (FATF) دوراً حاسماً في صياغة المعايير التنفيذية الدولية لمكافحة غسل الأموال وتأمين الأصول الافتراضية، وقد أصدرت المجموعات التوصية رقم (15) وتحديثاتها المؤطرة لما يُعرف بـ "قاعدة السفر (Travel Rule)، والتي تلزم كافة منصات ومزودي خدمات الأصول الافتراضية على مستوى العالم بجمع وتبادل معلومات المستثمر والمرسل إليه عند تنفيذ أي نقل لأصول مشفرة تتجاوز حداً مالياً معيناً، وذلك بغرض إنهاء حالة التخفي الحصري في التحويلات المشفرة²⁵.

ويتجلى التعاون القضائي الدولي عملياً من خلال الإنابات القضائية الدولية (Letters Rogatory) وطلبات المساعدة القانونية المتبادلة (MLATs) لضبط الأدلة الرقمية والاستماع للشهود وتجميد الحسابات البنكية المحفوظة بالخارج²⁶، وترتبط هذه الأطر أيضاً بالقواعد المنظمة لاسترداد الأصول والممتلكات الإجرامية الناتجة عن الجرائم السيبرانية وفقاً لأحكام اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود (اتفاقية باليرمو) واتفاقية الأمم المتحدة لمكافحة الفساد²⁷.

ورغم وجود هذه المنظومة الدولية، إلا أنها تعاني من بطء الإجراءات الإدارية والقوانين المعقدة للإنابات القضائية التقليدية التي قد تستغرق شهوراً طويلة، في حين أن عملية نقل وتبييض الأموال الرقمية تتم في ثوانٍ²⁸، ويضاف إلى ذلك تعقيد الرضا المستند إلى مبدأ التجريم المزدوج (Dual Criminality)، حيث تفرض بعض الدول الاستجابة للإنابة القضائية إذا كان الفعل السيبراني أو المالي غير مجرم في نظامها الداخلي، مما يجعل من توحيد المفاهيم التشريعية مطلباً لنجاح الإنابات القضائية الدولية²⁹.

²³ - أبو الفتوح، عبد الفتاح. م س

²⁴ - Council of Europe. (2001). Convention on Cybercrime (Budapest Convention). European Treaty Series - No. 185, Budapest.

²⁵ - Financial Action Task Force (FATF). (2023). Updated Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers. FATF Publications, Paris.

²⁶ - Council of Europe. Op.cit.

²⁷ - Financial Action Task Force (FATF). (2023). Updated Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers. FATF Publications, Paris.

²⁸ - Council of Europe. Op.cit.

²⁹ - Casey, E. (2020). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (4th ed.). Academic Press, San Diego.



المحور الثاني: الآليات الأمنية والتحديات العملية في مواجهة غسل الأموال الإلكتروني

إذا كانت الأطر التشريعية والقواعد القانونية تُوفر الغطاء الإجرائي والموضوعي للردع الجنائي، فإن كفاءة المواجهة تتوقف بالدرجة الأولى على مدى جاهزية وفاعلية الأجهزة الأمنية والتقنية، فالجريمة السيبرانية وغسل الأموال الرقمي يتعاملان مع معطيات رقمية غير مادية تتطلب أدوات أمنية وآليات فحص متقدمة قادرة على التكيف مع التطور السريع للتكنولوجيا.

ويتطلب البعد الأمني في هذا المجال الدمج بين التحري الجنائي التقليدي وتوظيف أحدث حلول التحقيق الرقمي واستخبارات البلوكشين وتطبيقات الذكاء الاصطناعي، وتتيح هذه الوسائل الأمنية المتطورة رصد التحركات المشبوهة وتتبع الأثر الرقمي للأموال الملوثة قبل تدويرها نهائياً وصعوبة استردادها.

ومع ذلك، يصطدم العمل الميداني الأمني بعقبات تقنية وجغرافية وتكتيكية بالغة التعقيد، تتراوح بين استخدام تقنيات التشفير المعقدة ودول الملاذات الآمنة، إلى ضعف التعاقد الدولي وتبين التشريعات الوطنية، ومن هنا يبرز المحور الثاني لتقييم القدرات التشغيلية والتحديات الواقعية التي تواجه جهود إنفاذ القانون.

ولبناء رؤية متكاملة حول هذه المواجهة الميدانية، سينقسم هذا المحور إلى مطلبين متكاملين: يستعرض المطلب الأول موضوع "المنظومات والآليات الأمنية والتقنية في تتبع الجرائم الإلكترونية ورصد الأموال المهربة"، بينما يحلل المطلب الثاني موضوع "التحديات والإكراهات الميدانية التي تواجه مكافحة الإجرام السيبراني وغسل الأموال الرقمي".

المطلب الأول: المنظومات والآليات الأمنية والتقنية في تتبع الجرائم الإلكترونية ورصد الأموال المهربة

تستوجب الطبيعة الفنية الشديدة للجرائم السيبرانية إعادة تشكيل منظومة العمل الشرطي والأمني، وتأهيل كوادر بشرية تمتلك خبرات مزدوجة تجمع بين العلوم الجنائية والعلوم المعلوماتية، فالتعامل مع هذا النمط الإجرامي لم يعد ممكناً بالأدوات التحقيقية التقليدية التي تعتمد على المعاينة المادية المباشرة.

وفي هذا الصدد، أصبحت علوم التحقيق الجنائي الرقمي (Digital Forensics) ركيزة رئيسة للأجهزة الأمنية لمداومة البيئات الرقمية، واستخلاص الأدلة الرقمية من الوسائط المخزنة أو الذاكرات المتطايرة، وضمان قبولها قضائياً وفق معايير علمية صارمة تحافظ على سلامة الشفرات الحسابية والدليل الرقمي.

وفي السياق ذاته، أدى تطور أساليب غسل الأموال الرقمية إلى الاستعانة بحلول تكنولوجية أكثر تعقيداً تعتمد على الذكاء الاصطناعي، وتحليل البيانات الضخمة، واستخدام أدوات تتبع سلاسل الكتل (Blockchain Analytics)، وتسهم هذه المنظومات التقنية في رصد المحافظ المشبوهة وربط المعاملات الرقمية بالهويات الحقيقية لمركبي الجرائم.

ولإبراز هذا الدور الأمني والتكنولوجي المتقدم في إنفاذ القانون، يُقسم هذا المطلب إلى جانبين رئيسيين: يستعرض أولاً دراسة "دور أجهزة الأمن المختصة والتحقيق الجنائي الرقمي (Digital Forensics) في جمع الدلائل"، بينما يركز ثانياً على فحص "التحديات المالية وتوظيف الذكاء الاصطناعي وتقنيات تتبع سلاسل الكتل (Blockchain)".

أولاً: دور أجهزة الأمن المختصة والتحقيق الجنائي الرقمي (Digital Forensics) في جمع الدلائل.

في جمع الدلائل تمثل الأجهزة الأمنية المختصة بالجرائم السيبرانية (Digital Forensics) خط الدفاع الأول في مواجهة الجرائم الرقمية وعمليات غسل الأموال المقترنة بها، وقد فرض التحول الإجرامي الرقمي على المؤسسات الأمنية إعادة هيكلة وحداتها وتأسيس



أقسام شرطية متخصصة ومجهزة بفرق استجابة سريعة للطوارئ السيبرانية (CERT/CSIRT) تمتاز بقدرات تقنية عالية لمراقبة حركة الشبكات، ورصد الهجمات، وتتبع الأنشطة المالية المشبوهة في الغرف المغلقة وعلى شبكات مظلمة مثل (Dark Web).³⁰

ويُشكل التحقيق الجنائي الرقمي (Digital Forensics) الأداة الأمنية المحورية للتعامل مع الأدلة الإلكترونية ذات الطبيعة المتقلبة والسريعة الزوال، ويتضمن هذا التحقيق منهجية صلبة لجمع واستخلاص وتحليل البيانات الرقمية الموجودة على الأجهزة المضبوطة، أو الخوادم السحابية، أو الذاكرة العشوائية (RAM)، وذلك بالاعتماد على برمجيات وتقنيات فحص تضمن حفظ الدليل الرقمي دون تغيير شفرته الهاشمية (Hash Value) لضمان حجته ومقبوليته أمام الهيئات القضائية.³¹

وتعمل الفرق الأمنية المتخصصة في الاستدلال الرقمي على اختراق منصات التواصل السرية واستعادة البيانات المحذوفة والرسائل المشفرة المخزنة في وسائط التخزين المتنوعة للجنة، ويمكن التفتيش الفني للذاكرة الحية للجهاز المضبوط من كشف المفاتيح الخاصة (Private Keys) المحفورة مؤقتاً في الذاكرة، مما يتيح للأجهزة الأمنية فتح المحافظ المشفرة للجنة والوصول المباشر للأموال الرقمية المهربة وتجميدها قبل نقلها إلى عناوين أخرى.³²

كما تعتمد هذه الوحدات الأمنية على مهارات الهندسة العكسية (Reverse Engineering) للبرمجيات الخبيثة المستخدمة في الهجمات، لمعرفة بنية الكود البرمجي وكيفية توجيه الأموال المنهوبة أو التعرف على خوادم التحكم والسيطرة (C2 Servers) المعنية بتلقي الأموال، وكفاءة عملية الجمع والأرشفة الفنية للدليل الرقمي تُشكل العامل الحاسم في نجاح تحويل الشبهات الأمنية إلى إدانات قضائية محكمة ومصادرة فعلية للأصول المكتسبة إجرامياً.³³

ثانياً: التحريات المالية وتوظيف الذكاء الاصطناعي وتقنيات تتبع سلاسل الكتل (Blockchain).

تحولت التحريات المالية الرقمية من أسلوب المراقبة المستندة البسيطة إلى الاستعانة بالتقنيات البرمجية المتقدمة لمواجهة السرعة الفائقة لغسل الأموال عبر الإنترنت، وفي هذا السياق، تلعب وحدات الاستخبارات المالية (FIUs) دوراً محورياً عبر تحليل قواعد البيانات الضخمة التي تردها من المؤسسات المالية والبنكية، واستخدام أنظمة الفرز الذكية لتصنيف مستوى الخطورة الخاص بالحسابات والأشخاص ورصد الأنماط المالية الشاذة غير المتوافقة مع السلوك المالي الطبيعي للعملاء.³⁴

ولمواجهة تخفي المعاملات عبر التشفير، طورت الأجهزة الأمنية ومؤسسات التحقيق المالي أدوات تتبع متخصصة في تحليل سجلات البلوكشين (Blockchain Analytics Tools) كبرمجيات (Chainalysis) و (Elliptic)، وتعتمد هذه البرامج التقنية على خوارزميات مسح البلوكشين العام لربط العناوين الرقمية المشفرة المجهولة بالكيانات الحقيقية ومزودي الخدمات الماليين والمعاملات الواقعية، من خلال تتبع خريطة التدفق المالي وتجميع العناوين المرتبطة بنسق إجرامي واحد في "عناقيد رقمية" (Clustering).³⁵

³⁰ - الشرقاوي، علي حسين. (2021). الأجهزة الأمنية والتحريات الرقمية في مواجهة الجريمة المنظمة السيبرانية. دار المعارف، القاهرة -

³¹ - Sammons, J. (2016). The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics (2nd ed.). Syngress / Elsevier, Waltham.

³² - الشرقاوي، علي حسين. م.س.

³³ - Sammons, J. op.cit.

³⁴ - Levi, M., & Reuter, P. (2021). Money Laundering Detection via Artificial Intelligence: Capabilities and Limits. Crime, Law and Social Change, 75(4), 411-432.

³⁵ - Albrecht, C., & Duffin, K. (2024). Blockchain Forensics: Tracing Virtual Assets in Complex Cybercrime Investigations. Security Journal, 37(1), 104-128.



كما يتصاعد الاعتماد على تقنيات الذكاء الاصطناعي (AI) وتعلم الآلة (Machine Learning) في بناء نماذج تنبؤية قادرة على كشف عمليات غسل الأموال في الوقت الفعلي (Real-time Detection)، وتستطيع شبكات الذكاء الاصطناعي فحص ملايين المعاملات المالية في الثواني، واكتشاف الأساليب المستحدثة مثل تفتيت المعاملات، أو التحويل المعقد بين منصات التداول المتقاطعة، فضلاً عن تحديد المحافظ المالية المشتبه في ارتباطها بأسواق الشبكة المظلمة (Darknet Markets) بشكل آلي³⁶.

وتتيح هذه الحلول التقنية المتقدمة للأجهزة الأمنية توفير خريطة مرئية متكاملة لخط سير الأموال الملوثة منذ لحظة سرقتها أو جنيتها من الجريمة السيبرانية وصولاً إلى محاولة تسهيلها في المنظومة المصرفية التقليدية، وبذلك تتحول التحريات الرقمية من مجرد رد فعل لاحق للجريمة إلى أداة أمنية استباقية تمكن من فرض التجميد الحفظي على الحسابات الرقمية المشبوهة وإجهاض عمليات التدوير في مراحلها الأولى³⁷.

المطلب الثاني: التحديات والإكراهات الميدانية التي تواجه مكافحة الإجرام السيبراني وغسل الأموال الرقمي

رغم التطور الملحوظ في المنظومات الأمنية واستخدام التقنيات الحديثة، إلا أن الساحة الميدانية لمكافحة الجريمة السيبرانية وتتبع الأموال الإلكترونية المهرة تصطدم بعقبات تقنية متصاعدة، فمع كل أداة أمنية مستحدثة، تُطور الشبكات الإجرامية تقنيات مضادة تعطل عمل فرق التحقيق الجنائي الرقمي.

وتأتي التحديات الفنية المرتبطة بالتشفير القوي استخدام خدمات التخفي واستعمال الخوادم الموزعة عشوائياً في مقدمة هذه الإكراهات، إذ تقف السلطات الأمنية عاجزة في كثير من الأحيان أمام فك تشفير البيانات أو تحديد الموقع الجغرافي الفعلي للجنة والهيكل الرقمية المستهدفة، فيما يُعرف بمشكلة "التعتيم الرقمي".

وعلى النطاق الميداني الدولي، يتفاقم الوضع نتيجة تباين التشريعات الوطنية وتوفر بيئات قانونية رخوة في بعض الدول تُسمى بملاذات التشفير، ويرافق ذلك ضعف التنسيق والتباطؤ الإداري في تبادل المعلومات بين الدول، ناهيك عن التجاذبات الجيوسياسية التي تحول دون تسليم المجرمين أو تجميد أصولهم المشبوهة.

ولسبر أغوار هذه العقبات والموانع الميدانية التي تُحد من كفاءة أجهزة الإنفاذ، يُطرح هذا المطلب عبر قسمين تفصيليين: يتناول أولاً بحث "العوائق التقنية المرتبطة بالتشفير، وصعوبة تحديد الهوية، وتحديد الاختصاص القضائي"، ثم يدرس ثانياً موضوع "رهانات غياب التنسيق الدولي وتباين التشريعات الوطنية بين دول ملاذات التشفير".

أولاً: العوائق التقنية المرتبطة بالتشفير، وصعوبة تحديد الهوية، وتحديد الاختصاص القضائي.

تُمثل أدوات التشفير القوية (Strong Encryption) وتطبيقات الاتصال والتخزين المعتمدة على خوارزميات التشفير بين الطرفين (End-to-End Encryption) العقبة التقنية الأكثر تعقيداً أمام أجهزة إنفاذ القانون. إذ يتعذر على المحققين الأمنيين قراءة محتوى الاتصالات المتداولة أو الوصول إلى البيانات المالية المخزنة داخل المحافظ المشفرة والهواتف الحديثة بدون المفاتيح السرية، حتى وإن تم الحصول على إذن قضائي بالتفتيش والتنصت، وهو ما يُعرف أمنياً بمشكلة "التعتيم الرقمي" (Going Dark)³⁸.

ويتفاقم هذا العائق التقني في ظل توظيف الجناة لشبكات التخفي مثل شبكة (Tor) والشبكات الخاصة الافتراضية (VPNs) التي تقوم بتوجيه حركة البيانات عبر سلسلة من الخوادم الموزعة عشوائياً حول العالم مع تشفير البيانات في كل محطة، وتؤدي هذه التقنيات

³⁶ – Levi, M., & Reuter, P. op.cit.

³⁷ – Albrecht, C., & Duffin, K. op.cit.

³⁸ – Kerr, O. S. (2021). Cross-Border Digital Searches and Jurisdiction in Cybercrime Investigation. Harvard Law Review, 134(6), 1950–1991.



إلى إخفاء عنوان البروتوكول الأصلي (IP Address) للمستخدم، وتجعل تحديد موقع الجاني الجغرافي أو الهوية الحقيقية لمرتكب عملية غسل الأموال أمراً معقداً يتطلب موارد فنية هائلة وقد لا ينتهي لنتيجة حتمية³⁹.

وعلى جانب آخر، تفرض الطبيعة العابرة للحدود للفضاء السيبراني تعقيدات جسيمة تسمى "معضلة تنازع الاختصاص الإقليمي والقضائي"، فالجريمة قد تُخطط في دولة، وتنفذ عبر خوادم ومعدات سحابية في دولة ثانية، وتصيب ضحايا في دولة ثالثة، بينما تتدفق الأموال المغسولة عبر منصات في دول رابعة وخامسة⁴⁰، وهذا التشتت الجغرافي يجعل من الصعب تحديد المحكمة المختصة قانوناً بالنظر في الدعوى، وتحديد أي قانون إرائي يجب تطبيقه لضبط الأدلة الرقمية الموجودة على خوادم أجنبية⁴¹.

إضافة إلى ذلك، فإن اللجوء إلى تقنيات "الحوسبة السحابية الموزعة" يتيح للشركات والكيانات الإجرامية تخزين البيانات بشكل مقطع في مراكز بيانات متعددة حول العالم، مما يعني أن طلب تفتيش خادم في دولة ما قد لا يُمكن المحققين من الوصول إلا إلى جزء لا قيمة له من الملفات المشفرة، الأمر الذي يصدم العمل الشرطي والقضائي بعوائق سيادية وفنية غير مسبقة⁴².

ثانياً: رهانات غياب التنسيق الدولي وتباين التشريعات الوطنية بين دول ملاذات التشفير.

يشكل التباين التشريعي بين الدول أحد أبرز الثغرات القانونية التي تستغلها الشبكات الإجرامية لتمرير الأموال المغسولة، فبينما تفرض الدول المتقدمة رقابة صارمة وقوانين متشددة على منصات العملات المشفرة وإجراءات الامتثال المالي، تعتمد دول أخرى تشريعات مرنة أو تفتقر تماماً للنصوص التي تنظم الأصول الافتراضية، فتتحول تلك الدول إلى "ملاذات آمنة للتشفير (Crypto Havens)" تجذب أنشطة غسل الأموال ومؤسسات الصرافة المشبوهة⁴³.

ويرتبط هذا التباين بتعثر مسارات التنسيق الدولي وتأخر الاستجابة لطلبات التعاون القضائي والأمني المتبادل، ففي كثير من الحالات، تستغرق الاستجابة للإبانات القضائية الصادرة لضبط أدلة مخزنة بالخارج عدة أشهر أو حتى سنوات بسبب التعقيدات البيروقراطية والنظم القانونية المختلفة، في الوقت الذي تستغرق فيه المعاملة المالية الإلكترونية المشبوهة ثوان معدودة لإتمامها ونقل الأموال إلى مكان آخر⁴⁴.

كما تبرز الخلافات السياسية والجيوستراتيجية بين الدول كعائق مانع أمام تبادل المعلومات الاستخباراتية المالية؛ إذ ترفض بعض الدول تسليم المجرمين السيبرانيين المقيمين على أراضيها أو الامتثال للنشرات الحمراء الصادرة عن منظمة الشرطة الجنائية الدولية (الإنتربول)، مما يوفر حصانة حقيقية للجنة ويحمي الأصول الرقمية المكتسبة إجرامياً من الملاحقة والمصادرة الدولية⁴⁵.

³⁹ – Maras, M. H. (2022). Cybercriminology: Theory, Research, and Practice. Jones & Bartlett Learning, Burlington.

⁴⁰ – Kerr, O. S. op.cit.

⁴¹ القاسمي، عبد العزيز. (2023). تحديات الاختصاص القضائي الجنائي في الفضاء السيبراني. المجلة الدولية للقانون، المجلد 12، العدد 1، ص ص 112-140.

⁴² – Maras, M. H. (2022). Cybercriminology: Theory, Research, and Practice. Jones & Bartlett Learning, Burlington.

⁴³ Casey, E. (2020). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (4th ed.). Academic Press, San Diego.

⁴⁴ – Interpol. (2023). Global Cybercrime Survey Report: Financial Cybercrime and Cross-Border Challenges. Interpol General Secretariat, Lyon.

⁴⁵ Casey, E. (2020). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (4th ed.). Academic Press, San Diego.



وأخيراً، أدى النقص الواضح في الموارد المادية والبشرية المتخصصة في كثير من الدول النامية إلى خلق حلقات ضعيفة في منظومة مكافحة الجريمة العالمية. تفتقر السلطات الأمنية والقضائية في هذه الدول للأدوات التقنية والتدريب اللازم لمحاربة التقنيات المستحدثة لغسل الأموال، مما يجعل الشبكة المالية الرقمية العالمية عرضة للاختراق والسيطرة من قبل تنظيمات الإجرام السيبراني المعقدة⁴⁶.

الخاتمة

أظهرت هذه الدراسة أن الجريمة السيبرانية وغسل الأموال الإلكتروني يشكلان نمطاً متطوراً منمط الإجرام المنظم الذي يتطلب استجابة قانونية وأمنية غير تقليدية، فالتحول الرقمي للخدمات المالية وفر للشبكات الإجرامية بيئة مثالية لعمليات غسل الأموال بسرعة فائقة ومعدلات مخاطرة منخفضة مقارنة بالطرق التقليدية.

إن مواجهة هذا التهديد تعتمد بالأساس على خلق توازن بين تحديث النصوص التشريعية الموضوعية والإجرائية من جهة، وتوفير البنيات الأمنية التقنية والكوادر البشرية المؤهلة من جهة أخرى، ولا يمكن للقانون وحده تدارك التطور التقني ما لم يُدعم بآليات أمنية تستند إلى أدوات التحقيق الرقمي والتنسيق المالي الاستخباري.

وتخلص الدراسة إلى أن رهان مكافحة الناجحة يظل مرهوناً بمدى توفر إرادة دولية حقيقية لتوحيد المعايير التشريعية وتفعيل اتفاقيات التعاون القضائي والأمني، وتسهيل تبادل المعلومات الفورية بين الدول لتجاوز العقبات الناتجة عن تعقيدات الجغرافيا وتشفير البيانات.

⁴⁶ – Interpol. (2023). Global Cybercrime Survey Report: Financial Cybercrime and Cross-Border Challenges. Interpol General Secretariat, Lyon.



المراجع والمصادر

المراجع العربية:

- أبو الفتوح، عبد الفتاح. المسؤولية الجنائية عن الجرائم السيبرانية وآليات مكافحتها: دراسة مقارنة. دار النهضة العربية، القاهرة(2021)..- سليمان، أحمد فاروق. غسل الأموال عبر الوسائط الإلكترونية والعملات الرقمية المشفرة. دار الفكر الجامعي، الإسكندرية(2020)..- المالكي، محمد الأمين. التحقيق الجنائي الرقمي والدليل الإلكتروني في المواد الجنائية. مجلة العلوم القانونية والأمنية، المجلد 5، العدد 2. (2022).

المراجع الأجنبية

- Brenner, S. W. Cybercrime: Criminal Threats to the Digital Age. ABC-CLIO / Praeger, Santa Barbara(2010).
- King, R., & Walker, C. Money Laundering in the Digital Era: Cryptocurrencies and Cybercrime Exploitation. Routledge, London(2019).
- United Nations Office on Drugs and Crime (UNODC). Comprehensive Study on Cybercrime and Electronic Financial Crimes. UN Publishing, Vienna(2021).