Tikrit University Journal of Law
Special Issue on the Fourth International Scientific Conference
(Prospects for Renewal and Innovation)
College of Law, Knowledge University
(30 April - 1 June -2025 A.D - Muharram 1447A.H)

ISSN: 2519 – 6138 (Print)
E-ISSN: 2663 – 8983(On Line)

TUJR
مجلة جامعة تكريت للحقوق
Tikrit University Journal for Rights

IRAQI Academic Scientific Journals
العراقية المجلات الاكاديمية العلمية

Tikrit University Journal for Rights
Journal Homepage : http://tujr.tu.edu.iq/index.php/t

كلية القانون
College of Law

Economic Crimes in the Era of Technological Revolution:Troubled Paths and Ongoing Challenges

Prof. Dr. Mustafa Ismail Al-Shamiya
Faculty of Law and Political Science, Lebanese University, Lebanon
alshamiehest@hotmail.com/Mobile

Article info.

Article history:
- Received 5 May 2025
- Accepted 1June 2025
-Available online 20 July 2025

Keywords:

Abstract: Economic crimes in the era of the technological revolution have significantly transformed with the rise of digital technologies. These crimes now include cyber fraud, hacking, identify theft, money laundering through cryptocurrencies, and intellectual property violations.

The rapid expansion of online platforms and digital currencies has provided criminals with new opportunities to exploit vulnerabilities, making detection and prosecution more challenging.

Major obstacles include the absence of a unified global legal framework, which complicates the ability of tackle cross-border crimes.

Jurisdictional issues further hinder enforcement, as criminals can evade justice by operating in countries with less stringent regulations. Moreover, technologies like blockchain provide anonymity, making investigations more difficult.

Law enforcement agencies often lack the necessary resources, expertise, and tools to effectively combat these crimes.

As technology continues to advance, the legal and regulatory systems must evolve to address these emerging challenges effectively.

مجلة جامعة تكريت للحقوق
العدد الخاص بالمؤتمر العلمي الدولي الرابع (أفاق التجديد والابتكار)
لكلية القانون - جامعة نولج
(٣٠ نيسان - ١ حزيران- ٢٠٢٥م-محرم ١٤٤٧)

الجرائم الاقتصادية في ظل الثورة التكنولوجية

مسارات متعثرة وتحديات مستمرة

أ.د. مصطفى إسماعيل الشامية

كلية الحقوق والعلوم السياسية ،الجامعة اللبنانية ،لبنان

alshamiehest@hotmail.com/Mobile

معلومات البحث :

تواريخ البحث:
- الاستلام : ٥/ آيار/ ٢٠٢٥
- القبول : ١ / حزيران/ ٢٠٢٥
- النشر المباشر: ٢٠/ تموز/٢٠٢٥

الكلمات المفتاحية :

الخلاصة: الجرائم الاقتصادية في عصر الثورة التكنولوجية قد تحولت بشكل كبير مع صعود التكنولوجيا الرقمية. تشمل هذه الجرائم الآن الاحتيال الالكتروني، والقرصنة، وسرقة الهوية، وغسل الأموال عبر العملات المشفرة، وانتهاك حقوق الملكية الفكرية. إن التوسع السريع في المنصات الرقمية والعملات المشفرة قد أتاح للمجرمين فرصاً جديدة لاستغلال الثغرات، مما جعل اكتشاف هذه الجرائم ومقاضاة مرتكبيها أكثر صعوبة.

تشمل العقبات الرئيسية غياب إطار قانوني عالمي موحد، مما يعقد القدرة على التصدي للجرائم العابرة للحدود. علاوة على ذلك، توفر تقنيات مثل البلوكشين مستوى من إخفاء الهوية، مما يصعب التحقيق في الجرائم.

مع تقدم التكنولوجيا، يجب أن يتطور النظام القانوني والتنظيمي للتعامل مع هذه التحديات حفاظاً على تكريس الاستقرار الاقتصادي والاجتماعي داخل الدول.

المقدمة: في العصر الحديث، أصبحت التكنولوجيا والمعلومات عناصر أساسية تؤثر بشكل كبير في مختلفة المجالات الاجتماعية والاقتصادية. ومع التطور المستمر للثورة الرقمية، شهدت إدارة الأنشطة الاقتصادية تحولات جوهرية، مما سهَّل وزاد من نسبة الجرائم الاقتصادية المرتكبة بأساليب متطورة ومعقدة في آنٍ معاً. فقد أدى هذا التقدم في تكنولوجيا المعلومات إلى تأثير مزدوج، فمن ناحية، وفرت أدوات متطورة لمكافحة الجرائم الاقتصادية، ومن ناحية أخرى، ساهمت في زيادة تعقيد وإخفاء هذه الجرائم عبر الوسائل الرقمية.

تشكل العلاقة بين الجرائم الاقتصادية وتكنولوجيا المعلومات محوراً جدلياً يتطلب دراسة معمقة لفهم أبعاده وانعكاساته على الأمن المالي والاقتصادي. فعلى الرغم من دور تكنولوجيا المعلومات في تسريع العمليات التجارية والمالية، إلا أنها وفرت أيضاً للمجرمين أدوات متقدمة لارتكاب جرائم مثل الاحتيال الالكتروني، وغسل الأموال، والتهرب الضريبي.

ومن هذا المنطلق، تهدف هذه الدراسة إلى تحليل كيفية استغلال التكنولوجيا في ارتكاب هذه الجرائم، مع تبيان السبل والوسائل الممكنة لاستخدامها في مكافحتها بفعالية.

في هذا السياق، يمثل الفضاء السيبراني أحد أبرز المفاهيم الحديثة التي أضافت بُعداً جديداً لعالم الجرائم الاقتصادية، فعلى الرغم من كونه أداة فعالة في مكافحة الجرائم المالية والاقتصادية من خلال تطوير أنظمة الحماية والرقابة الالكترونية، إلا أن الارتفاع المستمر في نسبة الجرائم السيبرانية التي تستهدف المؤسسات المالية والاقتصادية جعله ساحة صراع بين جهود مكافحة الجرائم الاقتصادية واستغلال التكنولوجيا في تنفيذها.

يُظهر الفضاء السيبراني كيف تستغل العصابات المنظمة التقنيات المتطورة في تنفيذ هجماتها، مثل الاختراقات الالكترونية، وقرصنة البيانات، واستغلال الثغرات في أنظمة الدفع الرقمية. وفي الوقت ذاته، يبرز دوره المحوري في ابتكار أنظمة متقدمة لرصد المعاملات المالية المشبوهة والكشف عنها، مما يجعله عاملاً حاسماً في تكريس الأمن المالي والاقتصادي.

تقدم هذه الدراسة رؤى تحليلية تهدف إلى تبيان آليات ووسائل تطور الجرائم الاقتصادية في عصر المعلومات، بغية تقديم حلول علمية وواقعية للتحديات المستجدة. كما تسعى إلى تسليط الضوء على كيفية استغلال التقنيات الحديثة لمكافحة الجرائم الاقتصادية المتزايدة.

سنحدد في ما يلي أبرز المرتكزات التي استندنا عليها لكتابة هذه الدراسة، وهي:

أولاً: سبب اختيار الدراسة.

يكمن السبب الجوهري والأساسي من وراء كتابة هذه الدراسة أهميتها وخطورتها في آن معاً، في العصر الحالي، حيث تتعدد أبعاد هذه الجرائم وتؤثر على كافة جوانب الاقتصاد الوطني والعالمي. كما أن هناك حاجة كبيرة للتفكير في إصلاحات قانونية وتطوير استراتيجيات رقابية لمكافحة هذه الجرائم، مما يجعل هذا الموضوع ذا أهمية كبيرة في البحث العلمي والتطبيق العملي.

ثانياً: أهداف الدراسة.

تهدف هذه الدراسة إلى:

١- تحليل العلاقة بين الجرائم الاقتصادية وتكنولوجيا المعلومات، ومدى تأثير هذه العلاقة على الأمن الاقتصادي.

٢- اختبار دور الفضاء السيبراني في مكافحة الجرائم المالية والاقتصادية.

٣- دراسة الأطر القانونية والتنظيمية لمكافحة الجرائم المالية في ظل التحديات التكنولوجية الحديثة.

٤- تقديم اقتراحات حول كيفية استغلال تكنولوجيا المعلومات والفضاء السيبراني في تحسين فعالية مكافحة الجرائم الاقتصادية.

ثالثاً: المناهج العلمية المتبعة.

من أجل الإحاطة بكل تفاصيل الدراسة بغية التوصل إلى نتائج علمية، آثرنا الركون إلى المناهج التالية:

١- المنهج التحليلي.

يعتمد هذا المنهج على تحليل البيانات والمعلومات المتاحة بهدف فهم الظواهر أو الموضوعات بشكل أعمق، وتفسير العلاقات بينها وبين العوامل المؤثرة فيها.

يهدف هذا المنهج إلى تحليل الأسباب والنتائج للظواهر التي يتم دراستها، وتقديم تفسير منطقي ومدعوم بالأدلة.

وتم الركون إليه في هذه الدراسة لتحليل التأثيرات الاقتصادية للفساد وتحليل مدى قدرة الأطر التقنية والقانونية في مكافحة الجرائم المالية والاقتصادية في ظل التطور المتسارع للتكنولوجيا.

٢- المنهج الوصفي.

يعتمد هذا المنهج على وصف الواقع بشكل دقيق، دون محاولة تفسير أو تعميم الظواهر. يتم جمع المعلومات المتعلقة بالجرائم الاقتصادية في الواقع، مع تقديم وصف مفصل للظواهر الاقتصادية المعنية.

لهذا استندنا إلى هذا المنهج لوصف الواقع وإظهار مدى تأثير التكنولوجيا سلباً وإيجاباً على الجانب الاقتصادي.

رابعاً: إشكالية الدراسة.

تدور هذه الدراسة حول إشكالية محورها: مدى تأثير التكنولوجيا الحديثة في توسيع نطاق الجرائم الاقتصادية، ومدى قدرة الفضاء السيبراني في أن يكون أداة فعالة في مكافحة هذه الجرائم.

وينبثق عن هذه الإشكالية الرئيسية مجموعة تساؤلات أبرزها:

١- ما هو مفهوم ومحددات الجرائم الاقتصادية التي ظهرت في العصر الحديث؟

٢- كيف تؤثر الثورة التكنولوجية على تطور الجرائم الاقتصادية؟
٣- كيف يؤثر استخدام العملات الرقمية في زيادة الجرائم الاقتصادية في عالم الذكاء الاصطناعي؟
٤- كيف يمكن للدول أن تتعاون دولياً لمكافحة الجرائم الاقتصادية التي تستخدم التكنولوجيا الحديثة؟
٥- ما هي أبرز التحديات القانونية التي تواجه محاربة الجرائم الاقتصادية الرقمية؟
٦- ما هي المخاطر المستقبلية للجرائم الاقتصادية نتيجة للتطورات التكنولوجية المستمرة؟

خامساً: فرضيات الدراسة.

آثرنا طرح عدة فرضيات في بداية الدراسة، ليصار في نهاية الدراسة إلى تأكيدها أو نفيها.

وتتمحور هذه الفرضيات حول ما يلي:

١- إن تطور تكنولوجيا المعلومات يعزز قدرة المجرمين على ارتكاب الجرائم الاقتصادية بطرق غير تقليدية، مما يزيد من تعقيد هذه الجرائم.
٢- إن الفضاء السيبراني يشكل منصة استراتيجية لكل من المجرمين والسلطات القانونية، وأنه إذا تم استغلاله بشكل صحيح، يمكن أن يصبح أداة هامة في مكافحة الجرائم الاقتصادية.
٣- إن التشريعات الحالية لا تتماشى مع تطور الجرائم الاقتصادية الرقمية، مما يستدعي تحديث الأطر الدستورية والقانونية لمواكبة الابتكارات التقنية المستخدمة في الجريمة.

سادساً: منهجية الدراسة.

تم تقسيم هذه الدراسة إلى قسمين، جاء القسم الأول تحت عنوان: "**محددات الجرائم الاقتصادية وسياق تطورها**" حيث توسعنا في القسم الأول في عرض وتحليل مفهوم الجرائم الاقتصادية وخصائصها ومدى تأثير استخدام العملات الرقمية في زيادة الجرائم الاقتصادية في عالم الذكاء الاصطناعي.

أما القسم الثاني فجاء تحت عنوان: "**الجهود الدولية لمواجهة الجرائم الاقتصادية في ظل التحديات المستمرة**".

بيَّنا في القسم الثاني أبرز الجهود الدولية لمواجهة الجرائم الاقتصادية والحد منها في ظل وجود تحديات على كافة الصعد، وحاولنا اقتراح كيفية الحد من هذه الجرائم الاقتصادية في عالم الغد، في محاولة للإجابة على السؤال المحوري في هذا الإطار، هل سيتم ضبط إيقاع تأثيرات التكنولوجية الحديثة السلبي في مجال الجرائم الاقتصادية أم سيزداد هذا التأثير مع ما يستتبع ذلك من تهديد للاستقرار الاقتصادي العالمي.

القسم الأول: محددات الجرائم الاقتصادية وسياق تطورها.

تعد الجرائم الاقتصادية بمختلف أشكالها من أخطر التحديات التي تواجه برامج التنمية والتقدم الحضاري في أي مجتمع، إذ تعيق النمو الاقتصادي وتلحق الضرر بالمصالح الوطنية، خاصة في ظل الانفتاح الاقتصادي والتطور السريع لمختلف مجالات الحياة. ومع الثورة التكنولوجية، ازدهرت التجارة الالكترونية وعولمة الاقتصاد، ما أدى إلى توسع نطاق الجرائم الاقتصادية.

ثمة جرائم تقليدية ذات تأثير اقتصادي، مثل السرقة، والاختلاس، والتزوير، والرشوة والابتزاز، والاحتيال، والتهرب الضريبي، والمماطلة في سداد الديون، حيث يتضرر منها الافراد بشكل مباشر، مما يعيق تحقيقهم للنمو الاقتصادي. إلا أن الجرائم الاقتصادية في جوهرها تستهدف السياسات الاقتصادية للدولة، مما ينعكس سلباً على الاستقرار المالي والاقتصادي للمجتمع بأسره.

وتتنوع الجرائم الاقتصادية من مجتمع لآخر تبعاً لاختلاف النظم الاقتصادية ومستوى التطور التكنولوجي. إلا أن وتيرة التطور السريعة التي يشهدها العالم أدت إلى ظهور أنشطة إجرامية جديدة، واتساع نطاق الجرائم الاقتصادية، مما يستدعي استراتيجيات متجددة وفعالة لمواجهتها.

المبحث الأول: مفهوم الجرائم الاقتصادية.

تتأثر طبيعة الجريمة الاقتصادية بشكل وثيق بالنظام الاقتصادي السائد في الدولة، حيث تلعب السياسات الاقتصادية والتشريعات التنظيمية دوراً محورياً في تشكيل أنماط وأساليب هذه الجرائم. ففي الاقتصادات الرأسمالية تنتشر جرائم مثل الاحتكار، وغسل الأموال، والتلاعب في الأسواق المالية، نتيجة لانفتاح الأسواق واعتمادها على المبادرات الخاصة والمنافسة الحرة. كما يشهد هذا النظام جرائم ذات طابع أكثر تعقيداً، مثل استغلال الأطفال في التجارة غير المشروعة، والتسبب في تلوث البيئة واختلال توازنها نتيجة السعي المستمر لتحقيق الأرباح دون مراعاة الأبعاد البيئية والاجتماعية.

أما الدول التي تتبنى النظام الاشتراكي، حيث تحتكر الدولة النشاط الاقتصادي، فإن الجرائم الاقتصادية الأكثر شيوعاً تشمل الرشوة، والاختلاس، وانتشار الأسواق الموازية وذلك نتيجة للقيود المشددة على الأسواق والموارد الاقتصادية.

ومع ذلك، هناك جرائم اقتصادية أخرى تتجاوز الفروقات بين النظامين الرأسمالي والاشتراكي، حيث تنتشر في كليهما جرائم مثل تجارة المخدرات، والتزوير، وجرائم الشيكات، والتدريس، والسرقات،

والنصب والاحتيال، إضافة إلى جريمة الربا في المعاملات المالية، مما يعكس الطبيعة المتغيرة والمترابطة للجريمة الاقتصادية في مختلف الأنظمة الاقتصادية[١].

ولو عدنا في قراءتنا وتحليلنا إلى تعاليم الدين الإسلامي في ما خص الجرائم الاقتصادية لوجدنا أنه حرّم جميع أشكال الكسب غير المشروع والخبائث وأخذ الأمور بغير حق. كما نهى عن كافة المعاملات التي تلحق الضرر بالفرد والمجتمع، تعزيزاً لمبادئ العدل والشفافية في التعاملات المالية. قال تعالى: (③♦🕔❄︎🕯︎❒③⑩♑︎⍓⍄✍︎✌︎ ✂︎✍︎✍︎✒︎⍋🔔♎︎⇦▫︎🙵 ↗◆✂︎✌︎♦✡⇖❑✂︎☎ ✍︎♦🕯︎▫︎▤→⧖□✡⬀❹♦🖃 📖❒✌︎⇘❑◆🕔◉♒︎♦▤↗☠ 🖃♦✡□⧖→💣 ✍︎♦▤↗❑♍︎🙵 📖❒♌︎ 🕗♦🖘 🕗♒︎✍︎✍︎♒︎⇘⧖♦🕔⮌♎︎✍︎⬀ ✌︎♎︎♑︎□🕔❷♦□🕔 ⇖♦♊︎ ✍︎♦❷♦✂︎⋎🖫 ✌︎♓︎♎︎☪▤↗☠⬁). وهذا التوجه الإلهي يرسخ قيم الأمانة والاستقامة في المعاملات الاقتصادية، مما يسهم في الحد من الجرائم الاقتصادية.

انطلاقاً من المحددات العامة والخاصة للجرائم الاقتصادية، بات بالإمكان إيجاد تعريف للجرائم الاقتصادية، فهو اصطلاحاً يستعمل للتعبير عن سلوك مخالف للقانون مستحقاً للعقاب لوقوع المخالفة على من يجرمه القانون، وبالتالي فإنها كل فعل غير مشروع يضر بالاقتصاد القومي بحال نص على تجريمه في قانون العقوبات أو القوانين الخاصة بخطط التنمية الاقتصادية الصادرة عن السلطة المختصة.

فالجرائم الاقتصادية الدولية يمكن اعتبارها أنها الأنشطة غير القانونية التي تتضمن الاستغلال غير المشروع للموارد الاقتصادية عبر الحدود الدولية، وتؤثر على الاقتصاد العالمي أو على الدول بشكل خاص. هذه الجرائم تشمل مجموعة من الأنشطة الاقتصادية التي لا تقتصر على الانتهاكات المحلية، بل تتعداها لتشمل الدول الأخرى، مما يجعل التحقيق والملاحقة الجنائية أكثر تعقيداً بسبب التداخل بين الأنظمة القانونية الدولية والمحلية، ولهذا تتطلب تعاوناً دولياً لمكافحتها.

المطلب الأول: خصائص الجرائم الاقتصادية.

يمكن تحديد مجموعة من الخصائص التي تميز الجرائم الاقتصادية والتي تجعلها أكثر تهديداً للأمن الاقتصادي والاجتماعي، نوردها في الفروع التالية:

الفرع الأول: اللامحدودية الجغرافية.

---

(1) Glaeser, Edward L., Sacerdote, Bruce. (2000). The Economic Approach to crime, Published by Elsevir, United States, PP: 30-32.

(٢) القرآن الكريم، سورة النساء، الآية ٢٩.

كانت الجرائم الاقتصادية قبل الثورة التكنولوجية محصورة في نطاقات جغرافية محددة، أما في العصر الحالي، فإن تطور الانترنت والأنظمة الرقمية أدى إلى زيادة هذه الجرائم بشكل كبير، حيث يمكن للمجرمين تنفيذ عملياتهم عبر الانترنت من أي مكان في العالم، وباتت الجرائم الاقتصادية عابرة للحدود. فالأفعال مثل غسل الأموال أو الاحتيال عبر الانترنت قد تحدث في دولة ما، بينما يكون المتضرر في دولة أخرى.

وتتعدد الأمثلة على اللامحدودية الجغرافية للجرائم الاقتصادية، وأبرزها:

- الهجوم على شركة **Sony** عام ٢٠١٤، حيث تعرضت شركة **Sony Pictures Entertainment** لهجوم الكتروني ضخم، حيث استطاع قراصنة تابعون لمجموعة تسمى **The Guardians of Peace** اختراق أنظمة الشركة وسرقة بياناتها. وهذا ما ألحق أضراراً كبيرة ليس فقط بالشركة نفسها بل بأسواق أخرى. فقد أثّر الهجوم على سلسلة التوريد العالمية للأفلام، وأدى إلى تسريب بعض الأفلام التي لم تكن قد تم إصدارها بعد[١].

الفرع الثاني: الجرائم الاقتصادية بين التعقيد المعرفي والتنوع.

تعتبر الجرائم الاقتصادية من الجرائم المعقدة التي تتطلب معرفة متخصصة في مجالات متعددة مثل الاقتصاد والتكنولوجيا والقانون.

غالباً ما يتم ارتكاب هذه الجرائم باستخدام أساليب متقدمة تتضمن التلاعب بالبيانات المالية، والتزوير والاحتيال عبر الانترنت.

وتتعدد الحالات والأمثلة على هذه الخاصية، وأبرزها: الاحتيال الالكتروني على البنوك.

في عام ٢٠١٦، تعرض بنك بنغلادش المركزي لعملية احتيال الكتروني ضخمة حيث تم اختراق النظام المصرفي للبنك وسرقة أكثر من ٨٠ مليون دولار. وتم تحويل الأموال إلى بنوك في دول مختلفة مما جعل من الصعب تتبع الأموال والقبض على الجناة.

جرى التحقيق في هذه الجريمة من قبل الشرطة المحلية في بنغلادش بالتعاون مع السلطات الأميركية وتم استخدام التكنولوجيا المتقدمة لتتبع مسار الأموال المهربة من خلال أنظمة الدفع الدولية مثل **SWIFT**.

([1]) Hern, A. (2014). "Sony Hack: How the Cyberattack Unfolded", www.theguardian.com, / technology/2014/dec/17/sony-hack-cyberattack-unfolded, date of visit to the website, 1/3/2025.

وعلى الرغم من كل الجهود في عملية التحقيق والتتبع إلا أنه لم يتم القبض على جميع المتورطين في هذه القضية.

تشمل الجرائم الاقتصادية مجموعة واسعة من الأنشطة غير القانونية التي تمس جميع قطاعات الاقتصاد، نذكر منها على سبيل المثال؛ غسل الأموال: هذه العملية تشكل إخفاء مصدر الأموال غير القانونية وتحويلها لتبدو كما لو كانت قد جاءت من مصادر مشروعة.

يتم ذلك عادة عبر سلسلة من المعاملات المالية المعقدة، مثل استخدام الشركات الوهمية، أو اللجوء إلى أنظمة مصرفية سرية، أو استغلال تقنيات حديثة مثل العملات الرقمية التي توفر درجة عالية من السرية وآثرنا ذكر قضية الحكومة الكندية والشركات الكندية عام ٢٠١٨ كمثال على قضية غسل الأموال ضمن خاصية التنوع وتعدد الجرائم الاقتصادية.

ففي تفاصيل هذه القضية أنه في عام ٢٠١٨، تم اكتشاف شبكة من الشركات الكندية التي كانت تستخدم حسابات مصرفية متعددة في مختلف دول العالم لغسل الأموال. تم تحويل هذه الأموال من خلال حسابات صورية وصرفها على مشاريع وهمية في عدة دول. وتم الكشف عن هذه الشبكة بعد تحقيقات أجرتها الشرطة الكندية بالتعاون مع الشرطة الدولية[١].

المطلب الثاني: آثار الجرائم الاقتصادية.

رمت تكلفة الجرائم الاقتصادية بثقلها على كافة قطاعات المجتمع نتيجة للتطورات المخيفة التي عرفها هذا النوع من الاجرام، والتي تظهر تجلياتها الاقتصادية والاجتماعية والأمنية سواء على المستوى الوطني أو على المستوى الدولي، وسنظهر فيما يلي هذه الآثار من خلال الفروع التالية:

الفرع الأول: الآثار العامة للجرائم الاقتصادية.

تترك الجرائم الاقتصادية آثاراً عميقة ومتعددة على مختلف جوانب المجتمع والاقتصاد. إن الآثار العامة للجرائم الاقتصادية تتعدى الاضرار الفردية لتشمل تأثيرات كبيرة على المجتمعات والاقتصادات الوطنية والعالمية. تلك الجرائم تؤدي إلى تدهور الثقة في النظام المالي والسياسي، وأبرز هذه الآثار العامة:

أولاً: التأثيرات على النظام السياسي.

([1]) Cyber Security in Canada Addressing the Growing Threat of Cybercrime". (2018). The Globe and Mail, www.theglobeandmail.com, date of visit, 25/1/2025.

يساهم الفساد المالي، وغسل الأموال، والرشوة في تقويض المؤسسات السياسية والحكومية وخاصة عندما يتم استخدام الأموال غير القانونية للتأثير على العمليات السياسية أو الانتخابية، مع ما يستتبع ذلك من تداعيات سلبية على مستوى العلاقات الدولية، فغسل الأموال والتهريب التجاري يهددان الأمن الاقتصادي العالمي، مما يعرض الدول للضغط من خلال العقوبات الدولية.

ثانياً: التأثيرات الاقتصادية.

تؤدي الجرائم الاقتصادية إلى تدمير الثقة في النظام الاقتصادي، مما يحد من الاستثمارات ويعطل الأنشطة الاقتصادية المشروعة.

وحسبنا في هذا المضمار أن فقدان عامل الثقة عند الشركات من قبل المستهلكين والمستثمرين يقلل فرص النمو الاقتصادي. بالإضافة إلى أن انتشار الجرائم الاقتصادية تؤدي إلى فقدان الثقة في المؤسسات المالية والمصرفية مما يسبب بانهيار لبعض المؤسسات المالية أو فقدان قيمة العملات المحلية.

ثالثاً: التأثيرات الاجتماعية.

تعزز الجرائم الاقتصادية ثقافة الفساد في المجتمع، وبالتالي يؤدي ذلك إلى انتشار سلوكيات غير قانونية بين الأفراد، مما يضر بالقيم الأخلاقية والاجتماعية، ويفاقم من معدلات الفقر والبطالة، فالشركات التي تتعرض للفساد أو الاحتيال المالي قد تضطر إلى تقليص العمالة أو حتى إغلاق مكاتبها وفروعها.

الفرع الثاني: الآثار الخاصة للجرائم الاقتصادية.

تتعدد الآثار الخاصة للجرائم الاقتصادية فمنها ما يندرج تحت إطار الآثار القانونية الخاصة، ومنها ما يندرج تحت الآثار النفسية والاجتماعية. وسنتوسع في الأقسام التالية في إيضاحها.

أولاً: الآثار القانونية الخاصة.

يواجه الأفراد والشركات التي ترتكب الجرائم الاقتصادية عقوبات قانونية قاسية يمكن أن تشمل هذه العقوبات غرامات مالية ضخمة، عقوبات سجن، وتجميد الأصول.

بالنسبة للشركات، قد يتضمن ذلك تجميد الأنشطة التجارية أو إغلاق الشركة نهائياً إذا ثبت تورطها في الأنشطة غير القانونية.

بالمقابل قد يضطر الأفراد أو الشركات المتضررة من الجرائم الاقتصادية إلى تقديم دعاوى قضائية للحصول على تعويضات مالية. تكاليف هذه القضايا يمكن أن تكون ضخمة، وقد تمتد لسنوات في بعض الأحيان قبل أن يتم الوصول إلى حكم نهائي[١].

ثانياً: الآثار النفسية والاجتماعية الخاصة:

يعاني الأفراد المتضررون من الجرائم الاقتصادية من التوتر والقلق والاكتئاب نتيجة لفقدان الأموال أو الوظائف أو المشاريع التجارية. قد ينتج عن ذلك تأثيرات طويلة المدى على الصحة النفسية، مثل القلق المزمن على المخاطر الاقتصادية المستقبلية. فضحايا العمليات الاحتيالية الكبيرة قد يواجهون صعوبة في استعادة ثقتهم بالأنظمة المالية، وقد يتطور ذلك إلى اضطرابات نفسية تؤثر على حياتهم الخاصة والمهنية.

كذلك يمكن أن تؤدي الجرائم الاقتصادية إلى صراعات بين الأفراد أو داخل المؤسسات. إذا كان الجناة هم أفراد قريبون من الضحايا مثل المديرين أو الشركاء، فإن ذلك قد يؤدي إلى تدهور العلاقات الشخصية والاجتماعية، حيث يصبح من الصعب التوفيق بين الأنشطة التجارية والأخلاقية.

ثالثاً: الآثار على الشركات والمؤسسات الخاصة:

تفقد الشركات والمؤسسات الخاصة المتورطة في الجرائم الاقتصادية حصتها في السوق لصالح المنافسين الأكثر نزاهة. فقد تتعرض لخسارة العقود والمشروعات، ما يؤدي إلى انخفاض مبيعاتها بشكل حاد بسبب فقدان العملاء والمستثمرين.

إن الشركات المتورطة في الجرائم الاقتصادية تجد نفسها مضطرة إلى وقف الأنشطة التجارية أو تعليق العمليات لفترة طويلة، ما يؤدي إلى تعطيل النمو. فالشركات التي تكون ضحية للاحتيال أو التلاعب المالي قد تضطر إلى تغيير هيكلها التنظيمي والمالي، ما يؤدي إلى تقليل قدرتها على التوسع[٢].

([1]) Levi, M. (2008). Organized Crime and the politics of Crime Control. In the Oxford Handbook of Criminology (4th ed., pp. 517-545).

([2]) Ibid.

المبحث الثاني: مقاربة تطور الجرائم الاقتصادية في ظل الذكاء الاصطناعي

إن التكنولوجيا بمختلف أشكالها والتي من بينها تقنيات الذكاء الاصطناعي هي سلاح ذو حدين، فهي تخدم الدول والمنظمات والشركات ومختلف شرائح المجتمع الدولي إذا استخدمت بمسارات إيجابية، ولكنها في ذات الوقت تشكل خطراً كبيراً عليهم إذا استخدمت بمسارات سلبية، بل تضرب أسس سياسات واقتصاديات الدول.

تشمل هذه الجرائم الاحتيال الالكتروني، حيث يقوم الجناة باستخدام البريد الالكتروني ومواقع الويب المزيفة لخداع الأفراد والشركات وسرقة أموالهم أو بياناتهم الشخصية.

بالإضافة إلى ذلك، ظهرت جرائم التصيد الاحتيالي التي تعتمد على إرسال رسائل الكترونية تبدو كأنها من جهات موثوقة لجمع بيانات حساسة مثل كلمات المرور والمعلومات المصرفية. كما ازداد نشاط القراصنة الذين يخترقون أنظمة الحواسيب التابعة للشركات والمؤسسات بهدف سرقة البيانات أو المال، مما أدى إلى زيادة الهجمات الالكترونية وإلحاق أضرار كبيرة بالشركات.

ثمة قضايا ومواضيع تدخل في صلب الجرائم الاقتصادية وتعقدت عملية رصدها ومتابعتها من قبل الجهات القانونية محلياً ودولياً في ظل الثورة التكنولوجية المتمثلة بصورتها الحديثة بالذكاء الاصطناعي، وسنتوسع في ما يلي في تحليل وعرض آلية وطرق استثمار الذكاء الاصطناعي من قِبَل المجرمين لتحقيق مآربهم.

المطلب الأول: الهياكل والأنظمة التكنولوجية المتبعة في الجرائم الاقتصادية:

في ظل التقدم التكنولوجي، ظهرت هياكل وأنظمة تكنولوجية متطورة أصبحت أدوات رئيسية في تنفيذ الجرائم المالية والاقتصادية. فقد استغل المجرمون التطورات التقنية لتصميم شبكات معقدة من البرمجيات الخبيثة، والذكاء الاصطناعي، وتقنيات التشفير، بهدف ارتكاب جرائم مثل الاحتيال المالي، وتبييض الأموال، واختراق الأنظمة المصرفية.

تعتمد هذه الهياكل على بيئات الكترونية خفية مثل الشبكة المظلمة **(Dark web)** والعملات المشفرة[*]، التي توفر سرية عالية وتساهم في تسهيل تنفيذ العمليات غير المشروعة بعيداً عن متابعة الجهات الرقابية.

---

[*] الشبكة المظلمة (Darkweb) هي جزء من الانترنت لا يمكن الوصول إليه باستخدام محركات البحث التقليدية مثل Bing أو Google، ولا يمكن تصفحه إلا عبر متصفحات مثل Tor، والتي توفر مستوى عالٍ من إخفاء الهوية والتشفير. أما العملات المشفرة (cryptocurrencies) هي أصول رقمية تعتمد على تقنيات التشفير لضمان الأمان وإدارة المعاملات، وتعمل بشكل لا مركزي عبر تقنية البلوكشين (Blockchain)، مما يجعلها مستقلة عن البنوك المركزية والحكومات. من أهم خصائصها، اللامركزية والتشفير والشفافية وقابلية التقسيم، أما أشهرها فهي، البيتكوين، الاثيرويم، الريبل، اللابتكوين، بينانس كوين.

في هذا السياق يصبح من الضروري فهم آليات هذه الأنظمة التقنية بشكل دقيق لتعزيز أساليب المكافحة، وتطوير استراتيجيات فعالة لحماية الاقتصاد من المخاطر المتزايدة المرتبطة بالجريمة السيبرانية.

الفرع الأول: بنوك الانترنت:

في سياق التطور التكنولوجي السريع وانتشار وتوسع شبكة الانترنت، نشأ ما يعرف ببنوك الانترنت أو البنوك الافتراضية أو الالكترونية.

هذه البنوك تعتبر وسيطاً للقيام بعدد من العمليات المالية والتجارية، حيث يقوم المستخدم بإدخال الشيفرة السرية على جهاز الكمبيوتر لتنفيذ التحويلات المالية المطلوبة. ويمكن اعتبارها بمثابة بوابات لتقديم كافة الخدمات المصرفية، الاستثمارية، والمالية عبر الانترنت في بيئة افتراضية، لكنها ليست بنوكاً بالمعنى التقليدي، حيث لا تقبل الودائع أو تقدم التسهيلات المصرفية أو غيرها من العمليات المصرفية المعتادة، ومن أبرز ميزاتها أن هذه البنوك أصبحت الوجهة المفضلة لمرتكبي الجريمة الاقتصادية، وخاصة مبيضي الأموال، وذلك لأنها توفر سرعة وأمان في نقل وتحويل الأموال مع ضمان السرية التامة للمستخدمين. فالمتعاملون مع هذه البنوك يظلون مجهولي الهوية، وتعمل هذه البنوك دون الخضوع لأي قوانين أو لوائح رقابية، مما يعزز من استخدامها في الأنشطة غير المشروعة.

كما أنها تقدم خدمات بنكية على مدار الساعة، مما يمكن العميل من الوصول إلى حسابه في أي وقت ومن أي مكان عبر الانترنت، ويشمل ذلك طلب أرقام معينة والتحقق منها باستخدام الرقم السري المقدم من البنك. هذه البنوك تسهل على مبيضي الأموال تنفيذ عمليات غسل الأموال من خلال تحويل الأرصدة عبر عدة بنوك حول العالم يومياً، مما يجعل تعقب هذه العمليات أو كشفها أمراً بالغ الصعوبة. وفي هذا السياق، تتخذ بنوك الانترنت ثلاثة اشكال رئيسية: الموقع المعلوماتي، الموقع الاتصالي، والموقع التبادلي[١].

الفرع الثاني: أنظمة التحويل الالكتروني للأموال.

يقصد بالتحويل المالي العملية التي يتم فيها قيد مبلغ من المال لصالح حساب معين، سواء كان ذلك في حساب الشخص نفسه أو في حساب شخص آخر. تتم عملية التحويل بناءً على طلب الشخص صاحب الحساب في البنك الذي يتعامل معه، سواء كان ذلك في نفس البنك أو في بنك آخر. في هذه العملية، يتم نقل الأموال من حساب إلى آخر، وقد تتطلب موافقة من الدائن أو العميل صاحب الحساب لتنفيذ التحويل، وتتم عادة باستخدام تقنيات مصرفية الكترونية حديثة تضمن الأمن والسرعة.

([1]) Kharouf, Omar M. (2020). "Digital Banking: Strategies for launching or Becoming a Digital Bank". Palgrave Macmillian, 2020, PP: 50-65.

يعتمد التحويل الالكتروني على العديد من الأنظمة المختلفة، ومن أبرزها نظام **"Fed Wire"** الذي يعد نظاماً داخلياً تابعاً للبنك الاحتياطي الفيدرالي في الولايات المتحدة الأميركية. عادة ما تتصل المؤسسات المالية بنظام **"Fed Wire"** عبر الهاتف لتقديم تعليماتها باستخدام بيانات مشفرة محددة تم الاتفاق عليها مسبقاً. يقوم هذا النظام **"Fed Wire"** بمضاهاة العبارة المشفرة التي تم تلقيها، ثم يعالجها الجهاز الالكتروني ويرسلها إلى الجهة المستلمة.

في حال كانت التحويلات المرسلة عبر **"Fed Wire"** موجهة إلى مؤسسة ليست على اتصال مباشر مع النظام، يتم قيد التحويلات فوراً في النظام، ويحظر المستلم بذلك إما عبر الهاتف من قبل **"Fed Wire"** أو من خلال إرسال صورة من إشارة التحويل إليها. وعادة ما يتم التحويل الفعلي للأموال في اليوم التالي من خلال نظام **"Fed Wire"** باستخدام أوراق البنك الاحتياطي الفيدرالي.

يعد هذا النظام **"Fed Wire"** أحد الأنظمة الآلية التي تعمل على مدار الساعة بشكل مستمر دون توقف، مما يعزز من سرعة وكفاءة العمليات المصرفية. من أبرز ميزاته توفير السرية العالية للعمليات المصرفية، إذ يتم تبادل الرسائل بسرعة فائقة، مما يساهم في تنفيذ التحويلات المالية بكفاءة وفعالية.

وهناك أيضاً نظام سيبس **CIPS** والذي ترجع ملكيته إلى القطاع الخاص بالولايات المتحدة الأميركية، فهو نظام المدفوعات بين البنوك لدار المقاصة، وهناك نظام سويفت **SWIFT** والمتمثل في شركة الاتصال المالية العالمية البنكية وهو الذي يعني جمعية الاتصالات السلكية واللاسلكية المالي الدولية عبر العالم.

لكن هذه الميزات نفسها تستغل من قبل مرتكبي الجرائم الاقتصادية، وعلى رأسها غسل الأموال حيث يتم تحويل أموال ضخمة إلى خارج الدولة بسرعة وبطريقة سرية، مما يصعب تتبع مصادرها أو كشف هوية الأطراف المتورطة. غالباً ما يتم توجيه هذه التحويلات إلى حسابات لشركات وهمية تقع في دول تتبنى أنظمة مصرفية تمنح سرية تامة لعمليات البنوك، مما يجعل من الصعب الاطلاع على دفاتر الحسابات أو تتبع حركة الأموال. هذه البيئة توفر ملاذاً آمناً للمجرمين لإخفاء أموالهم غير المشروعة وغسلها بعيداً عن أعين السلطات الرقابية[١].

([1]) Ibid, PP: 90-95.

المطلب الثاني: الوسائل القانونية التكنولوجية لممارسة الجريمة الاقتصادية.

لقد أصبح استخدام التكنولوجيا في الجرائم الاقتصادية أكثر تطوراً وتعقيداً مع مرور الوقت، مما يفرض تحديات كبيرة على الأنظمة القانونية والرقابة التقليدية. وبفضل تطور التقنيات القانونية والتقنية، بات المجرمون قادرين على استغلال الثغرات القانونية والفرص التي توفرها هذه التقنيات للتحايل على الأنظمة المالية. على سبيل المثال فإن **العقود الذكية** التي تستخدم في البلوكتشين[*] قد تُستغل في بعض الحالات لتمرير معاملات مالية مشبوهة دون الكشف عنها، بينما تُستخدم **الهوية الرقمية المزيفة** لتجنب التتبع والملاحقة القانونية.

كذلك، أصبحت بعض **المنصات الرقمية** والتطبيقات المالية تتيح للمجرمين إخفاء هوية المعاملات بسهولة من خلال تقنيات **التشفير** أو **إخفاء الهوية**، مما يجعل من الصعب كشف العمليات غير القانونية أو تتبع الأموال المشبوهة. وبالإضافة إلى ذلك، فإن غياب الرقابة الصارمة على هذه المنصات يمكن أن يشجع على انتشار **غسل الأموال** والاحتيال المالي عبر الإنترنت.

لمواجهة هذه التحديات، من الضروري تحديث وتطوير التشريعات القانونية لتواكب هذا التطور التكنولوجي، بحيث تشمل **تقنيات جديدة** مثل العقود الذكية، وتوفير إجراءات قانونية أكثر مرونة في مواجهة الجرائم الاقتصادية. كما يتطلب الأمر تعزيز التعاون بين الجهات **التشريعية** و**التقنية** لمكافحة استغلال التكنولوجيا في ارتكاب الجرائم الاقتصادية، وضمان وجود نظم فعالة لملاحقة المتورطين في هذه الأنشطة غير المشروعة.

---

[*] **العقود الذكية في البلوكشين (Smart contracts in Blockchain)** هو برنامج برمجي مخزن على شبكة البلوكشين، يُنفذ تلقائياً عند استيفاء شروط معينة، دون الحاجة إلى طرف ثالث أو وسيط.

مزايا العقود الذكية في البلوكشين:

- **الشفافية:** يمكن لأي شخص التحقق من العقد على البلوكشين.
- **الأمان:** لا يمكن التلاعب به بعد نشره.
- **السرعة والكفاءة:** لا حاجة إلى وسطاء، مما يقلل التكاليف والوقت.
- **عدم المركزية:** يتم تشغيل العقود عبر العقد (nodes) الموزعة في الشبكة.

الفرع الأول: التجارة الالكترونية.

التجارة الإلكترونية هي عملية شراء وبيع السلع والخدمات عبر شبكات الحاسوب المفتوحة مثل الإنترنت. كما تُعرف بأنها تنفيذ جميع العمليات المتعلقة ببيع وشراء البضائع والخدمات والمعلومات من خلال شبكة الإنترنت والشبكات التجارية العالمية الأخرى، بما في ذلك الإعلان، إتمام الصفقات، وتسوية المدفوعات المالية.

من خلال هذه التعريفات، يتضح أن الإنترنت يشكل محورًا رئيسيًا للتجارة الإلكترونية، حيث يُستخدم كوسيلة لممارسة الأنشطة التجارية عبر عمليات البيع والشراء. وهذه الخصائص توفر للمجرمين فرصة لارتكاب عمليات غسل الأموال، حيث يقومون بشراء سلع معينة وعرضها للبيع على مواقع الإنترنت بأسعار يحددونها بأنفسهم، وغالبًا ما تكون أعلى من قيمتها الحقيقية. الهدف من ذلك هو إعادة بيعها بعد شرائها، حتى وإن كان هامش الربح ضئيلًا أو حتى يتضمن خسارة. وبذلك، تُعتبر هذه الطريقة وسيلة لتمرير الأموال غير المشروعة وتحويلها إلى أموال مشروعة[١].

الفرع الثاني: وسائل الدفع الالكتروني.

تبعا للتطور التكنولوجي الذي ساهم بشكل كبير في تعدد وسائل الدفع الالكتروني فكانت هذه الوسائل المساعد للممارسة الجريمة الاقتصادية والمالية وهو ما سنعرضه كما يلي:

أولاً: النقود الالكترونية.

يطلق عليها النقود الرقمية هي المكافئ الالكتروني أو حافظات النقود الالكترونية للنقود التقليدية المعتاد تداولها وهى على عدة أشكال ، وكما ذكرنا سابقا فيعد الانترنت الأرض الخصبة التي من خلالها إجراء عمليات الشراء في ظرف قصير بدون عائق جغرافي أو مصرفي ، بحيث يتم تمرير النقود الالكترونية عبر شبكة الانترنت بصورة فورية دون الحاجة إلى وسيط مالي، ويستغلها مرتكبو الجريمة الاقتصادية والمالية لسببين، أولهما أن العملية الالكترونية تمتاز بالصعوبة لسرعة حركتها وتغييرها ، كما أن النقود الالكترونية تسهل عملية التحويل دون أي حماية أو وقاية، فمراحل غسل الأموال تصبح أسهل باستخدام النقود الالكترونية.

([1]) Laudon, Kenneth C., and Carol Guercio Traver. E-commerce: Business, Technology, Society. 15th ed. Pearson, 2021, Boston, MA. PP: 50-70.

ثانياً: بطاقة الائتمان.

يطلق عليها بطاقة الاعتماد أو بطاقة الدفع البلاستيكية، وهي عبارة عن مستند يعطيه مصدره لشخص طبيعي أو اعتباري بناءً على عقد بينهما يمكنه من شراء السلع والخدمات ممن يعتمد المستند دون دفع الثمن مباشرة لتضمنه التزام المصدر بالدفع ، ومن مظاهر ممارسة الجريمة الاقتصادية والمالية ببطاقة الائتمان التي تتيح دفع المال دون حيازته نقداً، إمكانية إيداع أموال طائلة بحساب البطاقة ويظل الحساب دائن فيتمكن المبيض من سحب الأموال النقدية أينما وجدت بالعالم.

ثالثاً: البطاقة الذكية والمعروف باسم Smart Card.

تقوم بصرف النقود التي كان قد سبق تحميلها مباشرة من العميل إلى القرص المغناطسي عن طريق ماكينة تحويل آلية، وتمتاز بعديد من الخصائص جعلها محل استخدام من قِبَل غاسلي الأموال ، فهي تشبه حافظة النقود الحقيقية التي يحملها الشخص وتضم أوراقا نقدية وعملة حقيقية ، فيمكن لمستخدم البطاقة أن يقوم بتحميل بطاقته إلى نقود عادية وما يطلق عليه عملية استعراض النقد من أي صراف ألي ، كما يمكنه سحب اعتمادات مالية الكترونية وعندما تتم عملية الشراء فالدفع يكون بخصم النقود الموجود قيمتها في البطاقة وهذه الوسيلة تشكل طريقة لغسل الأموال ، كما تمتاز البطاقة الذكية بعدة خصائص أخرى ، جعلتها مخرج لممارسة الجريمة الاقتصادية والمالية وخاصة غسيل الأموال.

رابعاً: الشيكات الالكترونية.

هي وثيقة الكترونية موثقة ومؤمنة، تحتوي على العديد من البيانات وتمتاز بعديد السمات، وتتجسد مظاهر ممارسة الجريمة الاقتصادية والمالية عن طريق هذه الوسيلة بحيث يكون الشيك الالكتروني هو وسيلة للتداول وكمثال على هذا، فإذا كان للشخص (أ) حساب لدى البنك وله مال غير مشروع من تجارة للمخدرات أو اختلاس، ويريد غسيله باستخدام الشيك، فعليه الدخول في معاملات مع أشخاص آخرين عن طريق الشيك، والتي قد تكون بيع أو إيجار أو قرض، فتتم عملية تحويل المال غير المشروع من ذمة (أ) إلى هؤلاء الأشخاص في مقابل الحصول على العقارات أو المنقولات المشروعة.

من خلال عرضنا لهذه الوسائل توصلنا إلى استخلاص نتيجتين أولهما أن الانترنت شكلت مرتعاً خصباً للممارسة الجرائم الاقتصادية والمالية بكل أشكالها وأهمها جريمة غسل الأموال، وان هذه الوسائل

تعتمد بشكل كبير على تقنيات الذكاء الاصطناعي لاحتوائها على أنظمة تكنولوجية متطورة جدا مما جعلها محل اهتمام ممارسي الجريمة الاقتصادية والمالية وبالخصوص غاسلي الأموال[١].

(١) Ibid.

القسم الثاني: الجهود الدولية لمواجهة الجرائم الاقتصادية في ظل التحديات المستمرة.

يمثل كل من التعاون الدبلوماسي والأمني الدولي لمكافحة الجرائم الاقتصادية دوراً أساسياً للحد من انتشار الجرائم الاقتصادية ومكافحتها.

ثمة صعوبة لتحديد إطار التعاون الدولي وأبعاده ويعود سبب ذلك إلى اتساع المجال والصور والأشكال التي يمكن أن يتخذها هذا التعاون، وعدم إمكان حصرها أو حصر الوسائل الجديدة والمتجددة التي تجعل هذا التعاون ظاهرة متغيرة ومتطورة بشكل مستمر، كذلك ارتباط هذا التعاون بمفاهيم الجريمة ومكافحتها، وهي مفاهيم يصعب معها وضع تصور محدد وإطار ثابت لأي منها.

المبحث الأول: الجهود الدولية لمكافحة الجرائم الاقتصادية الدولية.

ترافق مع التطور التكنولوجي وزيادة الجرائم الاقتصادية الدولية، جهود دولية لإيجاد بيئة دولية متعاونة تواكب الاستثمار السلبي للتكنولوجيا، وهو ما يساهم في تكريس الاستقرار الدولي على كافة المستويات. وكان للمعاهدات الدولية والمنظمة الدولية للشرطة الجنائية (الانتربول) مساهمات إيجابية في ردع ومكافحة هذه الجرائم.

المطلب الأول: دور المعاهدات الدولية في مكافحة الجرائم الاقتصادية.

أثمر الجهد الدولي منذ نهاية القرن العشرين إلى ظهور العديد من الاتفاقيات الدولية وأبرزها:

- اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، وقد تم التوقيع عليها في مدينة باليرمو (ايطاليا) عام ٢٠٠٠.
- الاتفاقية الأوروبية لمكافحة الإجرام المعلوماتي (بودابست) عام ٢٠٠١.
- اتفاقية الأمم المتحدة لمكافحة الفساد (٢٠٠٣).
- اتفاقية مجموعة الـ ٢٠ (G 20) لمكافحة غسل الأموال وتمويل الإرهاب (٢٠١٢).

يتبين للقارئ والباحث في مضمون هذه الاتفاقيات، وجود قواسم مشتركة عديدة لجهة مكافحة الجرائم الاقتصادية الدولية، والحد من انتشارها.

وسنحاول التوسّع في شرح مضمون كل من الاتفاقية الأوروبية لمكافحة الاجرام المعلوماتي (بودابست) عام ٢٠٠١ كنموذج أول، واتفاقية مجموعة الـ ٢٠ (G 20) لمكافحة الفساد (٢٠١٢) كنموذج ثانٍ للدلالة على الجهد الدولي المتخصص بالمعاهدات الدولية.

الفرع الأول: الاتفاقية الأوروبية لمكافحة الاجرام المعلوماتي – بودابست عام ٢٠٠١.

تعتبر اتفاقية بودابست (٢٠٠١) أول معاهدة دولية تهدف إلى مكافحة الجرائم المرتبطة بتكنولوجيا المعلومات على المستوى الدولي. تم إقرارها تحت إشراف مجلس أوروبا، وهي تمثل أطاراً قانونياً للتعاون بين الدول الأعضاء في مواجهة الجرائم التي تستخدم التكنولوجيا الحديثة، خاصة الانترنت كوسيلة ارتكاب.

تعكس هذه الاتفاقية التحديات الحديثة التي يواجهها النظام القانوني في التصدي للجرائم المعلوماتية التي يمكن أن تتجاوز الحدود الوطنية.

وإذا ما قمنا بتحليل أهدافها نخلص إلى أن الهدف الرئيسي لاتفاقية بودابست هو توحيد الإجراءات والتشريعات لمكافحة الجرائم الالكترونية على المستوى الدولي. فهي تسعى إلى توفير تعريفات قانونية موحدة للجرائم المعلوماتية، مثل القرصنة الالكترونية، الاحتيال الالكتروني، وغسل الأموال عبر الانترنت، مما يسهل التعاون بين الدول الأعضاء ويعزز قدرتها على التصدي لهذه الجرائم.

كذلك تهدف هذه الاتفاقية إلى تعزيز التعاون بين الدول لمواجهة التحديات التي تطرأ نتيجة لطبيعة الجرائم المعلوماتية العابرة للحدود، وإلى تطوير التشريعات الوطنية، وهذا يتطلب من الدول سن قوانين جديدة تعالج الجرائم الالكترونية، وتوفر الأدوات القانونية اللازمة لتحقيق العدالة وتطبيق القانون بشكل فعال على الجرائم التي تحدث في الفضاء السيبراني.

وتبرز عدة تحديات تواجه أهداف الاتفاقية، كالتطور السريع للتكنولوجيا. فمع مرور الوقت، تظهر تقنيات جديدة قد تكون خارجة عن نطاق الاتفاقية الأصلية. على سبيل المثال، تطور تقنيات الذكاء الاصطناعي والبلوكشين، وهذا ما يحتم تحديث وتفعيل بنود الاتفاقية بشكل دائم. بالإضافة إلى بروز تحديات تتعلق باختلاف الأنظمة القانونية بين الدول الأعضاء مما يؤدي أحياناً إلى صعوبة في تطبيق المعايير القانونية المنصوص عليها في الاتفاقية. فبعض الدول قد تملك قوانين أكثر مرونة في مجال الانترنت، في حين أن دولاً أخرى قد تكون أكثر تحفظاً وتحتاج إلى تعديلات قانونية لإدخال مفاهيم جديدة. وقد تواجه بعض الدول تصلباً في المواقف والتصرفات من دول أخرى فيما يتعلق بالتحقيقات الدولية أو تسليم المجرمين، خصوصاً في القضايا التي تشمل الأمن السيبراني أو الجرائم التي تتعلق بالخصوصية، ولكن على الرغم من كل تلك التحديات تعتبر اتفاقية بودابست أداة محورية لمكافحة الجرائم المعلوماتية على المستوى الدولي، حيث تساهم في توحيد الجهود الدولية لمكافحة الجرائم الالكترونية عبر الحدود وتعزيز التعاون القضائي بين الدول[١].

([1]) Council of Europe. Convention on Cybercrime (ETS No. 185). Strasbourg: Council of Europe, 2001, www.coe.int/ date of visit 3/3/2025.

الفرع الثاني: اتفاقية مجموعة الـ (٢٠) (G 20) لمكافحة غسل الأموال وتمويل الإرهاب ٢٠١٢.

تأتي هذه الاتفاقية في سياق الاهتمام العالمي المتزايد لمكافحة الأنشطة المالية غير المشروعة التي تؤثر على استقرار الاقتصاد العالمي وأمنه.

أقرت هذه الاتفاقية عام ٢٠١٢ في مدينة لوس كابوس في المكسيك.

تسعى الاتفاقية إلى تعزيز استخدام التكنولوجيا الحديثة لمكافحة غسل الأموال وتمويل الإرهاب. ويشمل ذلك استخدام التقنيات المتقدمة في مجال المراقبة والتحليل المالي. كذلك تعزز الاتفاقية دور منظمة العمل المالي **(FATF)** وهي الهيئة الدولية المسؤولة عن وضع المعايير والممارسات القانونية لمكافحة غسل الأموال وتمويل الإرهاب.

كما تتضمن الاتفاقية بنداً خاصاً بالعقوبات التي يمكن فرضها على الدول التي ترفض التعاون أو تتهاون في تطبيق القوانين التي تهدف إلى مكافحة غسل الأموال وتمويل الإرهاب.

تعمل الاتفاقية على خلق آلية رصد عالمية للمخالفات والتأكد من تنفيذ الإجراءات القانونية في جميع الدول الأعضاء[١].

المطلب الثاني: دور المنظمة الدولية في مكافحة الجرائم الاقتصادية الدولية:

الانتربول، أو المنظمة الدولية للشرطة الجنائية، هو جهاز دولي يضم في عضويته ١٩٥ دولة، ويهدف إلى تعزيز التعاون بين أجهزة الشرطة في جميع أنحاء العالم لمكافحة الجرائم بكل أنواعها، بما في ذلك الجرائم الاقتصادية.

يعمل "الانتربول" على تعزيز التعاون بين أجهزة الشرطة في الدول الأعضاء من خلال تبادل المعلومات وتحليلها للوقوف على أنماط الجرائم الاقتصادية مثل غسل الأموال والاحتيال المالي والتهرب الضريبي. ويساعد في تنسيق التحقيقات بين الدول لمكافحة الجرائم الاقتصادية العابرة للحدود، مما يسمح بتوجيه الجهود لملاحقة المتورطين عبر الدول المختلفة. كذلك يوفر الموارد التقنية للأجهزة الأمنية في الدول الأعضاء لمساعدتها في مكافحة الجرائم الاقتصادية.

يدير "الانتربول" قواعد بيانات تحتوي على معلومات عن المجرمين المطلوبين والأنشطة الاقتصادية غير القانونية. هذه القواعد تسهل تبادل المعلومات بين الدول وتساعد في اكتشاف المجرمين الذين يتنقلون بين الدول لتنفيذ أنشطتهم غير المشروعة.

([1]) Financial Action Task Force (FATF). 2012, The FATF Recommendations, Paris, France, 2012.

يقدم الانتربول برامج تدريبية وورش عمل للشرطة والسلطات المختصة في الدول الأعضاء لتطوير قدراتهم في مكافحة الجرائم الاقتصادية. هذه البرامج تشمل التدريب على التعرف على المعاملات المالية المشبوهة، تحليل الأدلة الرقمية، ومكافحة غسل الأموال.

وسنورد فيما يلي أبرز العمليات التي ساهم "الانتربول" فيها لمكافحة الجرائم الاقتصادية:

الفرع الأول: عملية "Sky Net"

بدأت هذه العملية عام ٢٠١٤، وهي استمرت في التطور مع مرور الوقت وأصبحت جزءاً من جهود الانتربول المستمرة لمكافحة الجرائم الاقتصادية عبر الانترنت، بما في ذلك غسل الأموال والأنشطة المالية غير المشروعة.

ساعدت عملية **Sky Net** في ملاحقة المجرمين الذين كانوا يديرون شبكات معقدة لغسل الأموال عبر الانترنت. وأسفرت الحملة عن اعتقال العشرات من الأفراد الذين كانوا يقفون وراء عمليات غسل الأموال. وتم استرجاع ملايين الدولارات التي كانت قد تم غسلها عبر منصات الانترنت، بالإضافة إلى إغلاق العديد من المنصات المالية غير القانونية التي كانت تستخدم في هذه الأنشطة[١].

الفرع الثاني: عملية "EMERALD"

هي عملية نظمها الانتربول عام ٢٠١٨ بهدف مكافحة الجرائم الاقتصادية وغسل الأموال. ركزت هذه العملية على استهداف الشبكات الاجرامية التي تستخدم وسائل تكنولوجية معقدة لغسل الأموال، بما في ذلك العملات المشفرة والأنظمة المصرفية غير الرسمية. هدفت العملية إلى تعزيز التعاون بين الدول الأعضاء في الانتربول للكشف عن عمليات غسل الأموال عبر الحدود وتقديم المجرمين إلى العدالة. وقد شاركت دول عديدة في هذه الحملة، منها دول متقدمة ومنها دول نامية، وأبرزها: الولايات المتحدة الأميركية والمملكة المتحدة وألمانيا وفرنسا وإيطاليا واسبانيا وهولندا والبرازيل وأستراليا والأرجنتين والبرتغال[٢].

كما شملت العملية أيضاً دولاً من افريقيا وآسيا والشرق الأوسط، حيث كانت تهدف إلى تحسين التنسيق بين أجهزة الشرطة الدولية في مكافحة الجرائم الاقتصادية العابرة للحدود.

---

(1) Interpol. (2014). Operating Sky Net: Coordinated international effort to Combat cybercrime. Lyon, France. www.interpol.int. date of visit, 7/3/2025.

(2) Interpol. (2018). Operating Emerald: Global Action Against the illicit Trafficking of Wildlife. Lyon: Interpol, 2018. www.interpol.int. date of visit 7/3/2025.

وأبرز ما حققتها هذه العملية هو اعتقال العديد من الأشخاص المتورطين في غسل الأموال والأنشطة المالية غير القانونية عبر الانترنت، واستعادة الأموال التي تم غسلها عن طريق تتبع المعاملات المالية وتحليل الروابط بين الحسابات[١].

المبحث الثاني: دور الذكاء الاصطناعي في مكافحة الجرائم الاقتصادية الدولية.

انطلاقاً من الحقيقة المسلَّم بها وهي أن الذكاء الاصطناعي سلاح ذو حدين، وبعد تطرقنا إلى الجانب السلبي في استخدام تقنيات الذكاء الاصطناعي في ارتكاب الجرائم المالية والاقتصادية في القسم الأول من هذه الدراسة، سنستعرض في هذا المبحث الجانب الإيجابي لتقنيات الذكاء الاصطناعي في مكافحة ومواجهة الجرائم المالية والاقتصادية من خلال الإجراءات الإدارية التكنولوجية لمكافحة الجرائم الاقتصادية في المطلب الأول، بينما خصصنا المطلب الثاني للإجراءات التقنية التكنولوجية لمكافحة الجرائم الاقتصادية.

المطلب الأول: الآليات الإدارية التكنولوجية لمكافحة الجرائم الاقتصادية.

في ظل تنامي الجرائم الاقتصادية وتزايد اعتمادها على التكنولوجيا، أصبح من الضروري تطوير آليات إدارية تكنولوجية فعالة لمكافحتها. وتتمثل هذه الآليات في اعتماد أنظمة متقدمة لمراقبة العمليات المالية، وتعزيز استخدام الذكاء الاصطناعي والتحليلات البيانية لاكتشاف الأنشطة المشبوهة، بالإضافة إلى تحسين البنية التحتية للأمن السيبراني في المؤسسات المالية والاقتصادية. كما يشمل ذلك التنسيق بين الهيئات الرقابية والبنوك المركزية من خلال منصات رقمية متكاملة تتيح تبادل المعلومات بسرعة وكفاءة.

إن توظيف التكنولوجيا في الإدارة الرقابية يسهم في رفع مستوى الشفافية، ويحسن الاستجابة للهجمات الالكترونية، ويعزز القدرة على تتبع التدفقات المالية غير المشروعة، مما يشكل رادعاً قوياً أمام مرتكبي الجرائم المالية والاقتصادية.

الفرع الأول: تأمين الأجهزة والبيانات.

إن أول خطوة احترازية في سبيل توفير الأمان هي تأمين الأجهزة، لن يتسنى هذا إلا من خلال تأمين المبنى وحصر الدخول إليه بالأشخاص المصرح لهم، ولن يتحقق هذا إلا باستخدام التكنولوجيا الحديثة للدخول على الأنظمة مثل بصمة الأصبع، بصمة العين، البطاقة الممغنطة، كما يجب أن يتم

([1]) Ibid.

تأمين البيانات من خلال صياغة الضوابط المنظمة لعمليات التشغيل ولمبرمجي قواعد البيانات ومدرائها وضبط إدارة شبكات وخطوط الاتصال، وعمليات الادخال والإخراج، والضوابط الأمنية لبناء وتشغيل البرامج التطبيقية.

نستشف من كل هذا أن عملية تأمين الأجهزة والبيانات هي عملية إدارية تكنولوجية تتطلب أشخاص يتمتعون بخبرة في المجال الإداري والتكنولوجي يخولهم القيام بهذه الإجراءات التي تشكل رادع في مواجهة مختلف الخروقات باستخدام تقنيات الذكاء الاصطناعي.

الفرع الثاني: تأمين الجانب البشري.

يتمتع مرتكبي الجرائم الاقتصادية الدولية، بمهارة وخبرة تكنولوجية عالية تمكنهم من ارتكاب هذه الجرائم بطرق معقدة.

ولذلك أصبح من الضروري التركيز على تدريب وإعداد العنصر البشري كآلية أساسية لمكافحة الجريمة الاقتصادية، وذلك من خلال اتخاذ مجموعة من الإجراءات الوقائية والتدابير العملية.

تتضمن هذه الإجراءات عقد ندوات ومؤتمرات ومحاضرات بشكل دوري في مجال أمن المعلومات، لتوعية الأفراد بأهمية حماية البيانات والمعلومات. كما يتم عرض نشرات داخلية وتعليمات إدارية تتضمن اطلاع الموظفين على المعلومات الأساسية المتعلقة بالأمن المعلوماتي. بالإضافة إلى ذلك، يتم إرسال الموظفين لحضور المعارض العلمية المتخصصة في الأجهزة والبرامج المتعلقة بالأمن وتنظيم دورات تدريبية متخصصة في هذا المجال لضمان أن الموظفين يمتلكون خلفية قوية حول كيفية الحفاظ على أمن المعلومات.

إلى جانب هذه الإجراءات، هناك خطوات إدارية وتكنولوجية يجب أن تتخذها الإدارة لضمان تأمين الجانب البشري، مثل منع التوظيف المؤقت الذي قد يعرض النظام للخطر. كذلك يجب إلزام الموظف بتسليم جميع المفاتيح والبطاقات الممغنطة التي كانت بحوزته عند انتهاء خدمته، مع تغيير كلمة السر قبل مغادرته.

كما يعتبر ربط الترقية بمستوى التزام الموظف بأمن المعلومات خطوة مهمة لضمان تحقيق الأمان داخل المؤسسة.

ولضمان استراتيجية أمنية قوية يصبح لزاماً على المؤسسات وخصوصاً المؤسسات المالية، إحداث دائرة أو مصلحة تضم متخصصين في المجال المعلوماتي من أهل الخبرة في معالجة البيانات

والبرمجة حسب نظم التشغيل ولغات البرمجة وقواعد البيانات المستخدمة في المؤسسة ومدربين على التنسيق الأمني ولديهم المقدرة الكافية للتعامل مع جرائم نظم المعلومات والحالات الطارئة[1].

المطلب الثاني: الآليات التقنية التكنولوجية لمكافحة الجرائم الاقتصادية الدولية.

في ظل التطور المستمر للجرائم الاقتصادية، أصبح من الضروري الاعتماد على الآليات التقنية والتكنولوجية لمكافحتها بشكل فعال.

وتشمل هذه الآليات استخدام الذكاء الاصطناعي وتحليل البيانات الضخمة لرصد الأنشطة المشبوهة والأنماط غير الطبيعية في العمليات المالية، مما يساعد على اكتشاف عمليات الاحتيال وغسل الأموال في مراحلها المبكرة.

كما أن توظيف تقنيات البلوكشين يعد من الحلول الفعالة لضمان الشفافية في المعاملات المالية، حيث توفر سجلاً لا يمكن التلاعب به، مما يحد من التزوير ويعزز الثقة في التعاملات المالية. بالإضافة إلى ذلك، تعزز أنظمة الأمن السيبراني من حماية البنى التحتية الرقمية من الاختراقات والهجمات الالكترونية التي قد تستهدف المؤسسات المالية.

كما أن البرمجيات المتخصصة في تتبع التدفقات المالية غير المشروعة تساهم في الكشف عن عمليات غسل الأموال والنشاطات المالية غير القانونية بشكل سريع ودقيق. إن تسخير التكنولوجيا الحديثة في مكافحة الجرائم الاقتصادية يعزز قدرة المؤسسات الرقابية على التصدي للتهديدات المتزايدة، ويضمن حماية الأنظمة المالية من الاستغلال غير القانوني، مما يساهم في تعزيز الاستقرار الاقتصادي وزيادة ثقة المستثمرين في الأسواق المالية.

الفرع الأول: الحماية الالكترونية.

تتمثل الحماية الالكترونية لجهاز الحاسوب في عدة إجراءات تهدف إلى الحفاظ على أمان البيانات والمعلومات، من أهم هذه الإجراءات: حذف الملفات غير الهامة والتأكد من عدم بقائها في سلة المحذوفات، تركيب برامج تمنع حذف أو مسح المعلومات من متصفح الانترنت أو المستكشف واستخدام برامج مخصصة لتخزين العمليات السابقة وكلمات المرور بشكل آمن. كما يستحسن تطبيق أنظمة حماية مرور قوية مع الحفاظ على تحديثات أمنية مستمرة لتفادي الثغرات التي قد يتسلل منها المهاجمون؛ من بين التدابير الأمنية الهامة للحفاظ على أمان الحاسوب عند الارتباط بالشبكات، هو التأكد من عدم وجود

([1]) Levi, M. (2008). PP: 508-515.

برامج تجسس مثل "طروادة"(*) التي قد تستغل الثغرات للوصول إلى البيانات الحساسة. إضافة إلى ذلك، يفضل من الناحية الأمنية عند استخدام الانترنت عدم حفظ كلمات المرور تلقائياً، مما يقلل من خطر سرقة البيانات في حال تم اختراق الجهاز. كما يُنصح بغلق المتصفح فوراً عند الانتهاء من استخدامه، لتعطيل خاصية الرجوع إلى الصفحات السابقة التي قد تحتوي على معلومات حساسة. أيضاً وفي إطار كشف عن الغش والاحتيال، اعتمد نظام تقييم الاحتيال **Fico-Falcon** الذي يعتمد على شبكة عصبية لنشر أنظمة الذكاء الاصطناعي المتطورة القائمة على التعلم العميق، وهو نظام يُعتمد في المجال المصرفي أيضاً وفي إطار الحماية الالكترونية. كما يجب تركيب البرامج المضادة للفيروسات على الجهاز وتشغيلها طوال فترة استخدام الجهاز [١].

الفرع الثاني: الحماية بواسطة التشفير.

يعد التشفير من الآليات التقنية التكنولوجية لمنع التنصت على إرسال البيانات عن طريق الشبكة، والمقصود بالتشفير هو تحويل المعلومات إلى شيفرات غير مفهومة وهذا لمنع الأشخاص غير المرخص لهم من الاطلاع على المعلومات أو فهمها، كما تعني عملية التشفير تحويل النصوص العادية إلى مشفرة بحيث تشكل شبكة الانترنت الوسيلة الأضخم لنقل المعلومات الحساسة. وللتشفير طرق منها الشهادات الرقمية، البصمة الالكترونية، والتوقيع الالكتروني واستخدام كلمات المرور تبعاً للمزايا التي تتمتع بها النظم المتخصصة، مثل القدرة على العمل بدون التعرض للنسيان، وتوثيق القرارات بشكل دائم، وإمكانية تجميع خبرات متعددة في نظام واحد؛ فإن نظام الذكاء الاصطناعي **"FinCEN" (FAIS)** يهدف إلى تحليل وتقييم التقارير المالية الكبيرة للكشف عن مؤشرات غسل الأموال. يُركّز على تحويل البيانات من منظور المعاملات حيث يهدف إلى تحليل وتقييم التقارير المالية الكبيرة للكشف عن مؤشرات غسل الأموال؛ كذلك يركز هذا النظام على تحويل البيانات من منظور المعاملات إلى منظور الأفراد أو الكيانات، مما يسهل ربط المعاملات ذات الصلة وتحديد الأنماط المشبوهة.

منذ تشغيله في عام ١٩٩٣، ساهم FAIS في معالجة حوالي ٢٠٠,٠٠٠ معاملة أسبوعياً، مما أدى إلى تطوير تقارير دعم تحقيقية تتعلق بأكثر من مليار دولار من الأموال المحتمل غسلها. بالإضافة إلى **FAIS**، أطلقت **FinCEN** مبادرة **FinCEN** للابتكار لتعزيز استخدام التقنيات الحديثة، بما في ذلك الذكاء الاصطناعي، في مكافحة الجرائم المالية. تتضمن هذه المبادرة برامج مثل "ساعات الابتكار"

(*) نظام تجسس طروادة: هو نوع من البرمجيات الخبيثة التي تم تصميمها لسرقة البيانات أو المعلومات الحساسة من جهاز الحاسوب دون أن يكتشف المستخدم ذلك.

(1) Fico. (2020). Fico Falcon Fraud Management: protecting business and consumers from financial fraud. Fico. San Jose, CA, USA, www.fico.com. Date of visit 4/3/2025.

(Innovation Hours)، التي توفر منصة للتواصل بين المؤسسات المالية ومقدمي التكنولوجيا لمناقشة الحلول المبتكرة في مجال مكافحة غسل الأموال وتمويل الإرهاب.

وقد ساعد هذا النظام على مدى سنتين في تحديد أكثر من ٤٠٠ حالة محتملة لغسل الأموال، مما يعكس فعالية الذكاء الاصطناعي في محاربة الجرائم المالية وتعزيز الأمان المالي؛ فالغاية من استخدام الأنظمة المتخصصة بتقنيات الذكاء الاصطناعي تكمن في تحسين وتعزيز عمليات المراقبة واتخاذ القرارات بشكل أكثر فعالية من قدرات خبراء أمن المعلومات التقليديين. هذه الأنظمة تساهم في تحسين قاعدة المعرفة المتعلقة بالتهديدات والسياسات والإجراءات والمخاطر الخاصة بأمن المعلومات، مما يسمح بتحليل البيانات بشكل أسرع وأكثر دقة، كما توفر القدرة على التنبؤ بالهجمات المستقبلية، وبالتالي تحديد طرق المعالجة والوقاية المناسبة قبل وقوعها. بهذا الشكل، تُعد هذه الأنظمة أداة قوية في التصدي للتهديدات الأمنية وضمان حماية الأنظمة المالية والمعلوماتية[١].

([1]) Kennes, S. & Radhakrishnan, S. (2021). Cryptography and its role in combating economic crimes: A modern approach. Switzerland, www.springer.com Date of visit 10/3/2025.

الخاتمة.

تُظهر هذه الدراسة الجرائم الاقتصادية في ظل **الثورة التكنولوجية** حجم التحديات التي تفرضها هذه الجرائم على **الأنظمة المالية والاقتصادات العالمية.** وبينما توفر **التكنولوجيا الحديثة** فرصاً هائلة في مكافحة هذه الجرائم، إلا أن هناك تهديداً دائماً يتمثل في **استغلال المجرمين** لهذه التقنيات لتطوير **أساليب إجرامية أكثر تعقيداً.** في مواجهة هذا التحدي المتزايد، تبرز **أهمية التشريع والتعاون الدولي** كعوامل أساسية لمكافحة الجرائم الاقتصادية بفعالية.

تعتبر **التشريعات** عنصراً أساسياً في هذا السياق، حيث يجب على **القوانين المحلية والدولية** أن تتطور لتواكب التغيرات السريعة في **التقنيات الحديثة.** من الضروري **تحديث القوانين المتعلقة بمكافحة الجرائم المالية** لتتناسب مع الابتكارات التكنولوجية، حيث أن **التشريعات القديمة** التي لا تراعي التحديات التكنولوجية تصبح عاجزة عن التعامل مع **الجرائم الاقتصادية الرقمية،** مما يفتح المجال أمام **المجرمين للاستفادة من الثغرات القانونية،** لذا تصبح الحاجة ملحة لتطوير **آليات قانونية مرنة** لمواكبة أساليب الجريمة الحديثة.

أما على مستوى التعاون الدولي، فهو يشكل ركيزة أساسية لمكافحة الجرائم الاقتصادية في العصر الرقمي، إذ أن هذه الجرائم غالباً ما تتجاوز الحدود الوطنية، مما يتطلب تنسيقاً مشتركاً بين الدول عبر تبادل المعلومات والخبرات، وتطوير سياسات عالمية لمكافحة الجرائم الاقتصادية، فيجب أن تركز **الاتفاقيات الدولية** على تعزيز التعاون بين الدول في مجال التحقيقات الجنائية، وتوحد التشريعات المتعلقة بالجرائم المالية الرقمية. كما ينبغي أن يشمل التعاون ليس فقط تبادل البيانات، بل وأيضاً تدريب **الكوادر المختصة في التحقيقات الرقمية والأمن السيبراني** لضمان قدرتهم على مواجهة الجرائم المتطورة.

على صعيد **استثمار الفضاء السيبراني والتكنولوجيا الحديثة** لمكافحة الجرائم المالية، ينبغي أن يكون هذا الاستثمار موجهاً نحو **حماية الأنظمة المالية** من الممارسات غير القانونية؛ فعلى الرغم من أن الفضاء السيبراني قد يصبح بيئة خصبة للأنشطة الإجرامية، إلا أنه يمكن أن يشكل أداة حاسمة في **التصدي للجرائم** إذا تم استغلاله بشكل صحيح.

من خلال **أدوات مثل الذكاء الاصطناعي وتحليل البيانات الضخمة،** يمكن للجهات المعنية رصد الأنماط المشبوهة في المعاملات المالية بشكل أسرع وأكثر دقة، كما يمكن أن تساهم **تكنولوجيا البلوكشين** في تعزيز **الشفافية والمساءلة** في المعاملات المالية، مما يزيد من قدرتها على منع الجرائم المالية.

في هذا السياق، تبقى **الجرائم الاقتصادية** في ظل **الثورة التكنولوجية** قضية معقدة تتطلب **تعاوناً وثيقاً** بين **الحكومات، المؤسسات المالية، والشركات التقنية** لضمان مواجهة هذه التحديات المستمرة حيث تتراوح الأضرار الناتجة عن هذه الجرائم بين **الخسائر المالية الكبيرة، فقدان الثقة في المؤسسات المالية،** والتأثيرات السلبية على **النمو الاقتصادي**؛ لذلك يجب أن نواجه هذه التحديات بشكل جماعي، من خلال **تطوير استراتيجيات جديدة** لمكافحة الجرائم الاقتصادية التي تستفيد من التقدم التكنولوجي، وفي الوقت ذاته، ضمان **استثمار هذه التقنيات** بشكل إيجابي للحفاظ على **الأمن الاقتصادي.**

الاستنتاجات التي يمكن استخلاصها من هذه الدراسة للإجابة على إشكالية الدراسة وتساؤلاتها يمكن إيجازها بالتالي:

١- الجرائم الاقتصادية قد استفادت بشكل كبير من الثورة التكنولوجية، حيث مكنت المجرمين من تنفيذ أنشطتهم بطرق أكثر سرية وتعقيداً، مما يتطلب تحديثاً مستمراً في استراتيجيات المكافحة.

٢- هناك ضرورة ملحة لتحديث الأطر القانونية والتشريعية لمواكبة التغيرات التكنولوجية، مع ضمان حماية الخصوصية والبيانات الشخصية في المعاملات المالية.

٣- الفضاء السيبراني، رغم كونه بيئة خصبة للجرائم المالية، يمكن أن يصبح في الوقت نفسه أداة أساسية في مكافحة هذه الجرائم إذا تم استغلاله بشكل صحيح وتطوير تقنيات جديدة للكشف عن الأنشطة المشبوهة.

٤- تبقى الجرائم الاقتصادية في ظل الثورة التكنولوجية قضية معقدة تتطلب تعاوناً وثيقاً بين الحكومات، المؤسسات المالية، والشركات التقنية لضمان مواجهة هذه التحديات المستمرة.

أما لجهة الرد على فرضيات الدراسة تبين لنا من خلال الدراسة، صحة ما طُرِح من فرضيات من منطلق العلاقة الطردية بين التطور التكنولوجي وزيادة قدرات المجرمين والأساليب المتبعة في ارتكاب الجرائم الاقتصادية، كذلك تبين أن ثمة علاقة عكسية بين تفعيل التشريعات الدولية والجرائم الاقتصادية وبالتالي كلما تم تفعيل التعاون التشريعي على المستويين الداخلي والدولي كلما انخفضت نسبة الجرائم الاقتصادية.

بناءً على ما تم مناقشته في هذه الدراسة حول الجرائم الاقتصادية في ظل الثورة التكنولوجية، وارتباطها بتكنولوجيا المعلومات والفضاء السيبراني، يمكن تقديم عدد من المقترحات العملية والفعالة لمكافحة هذه الجرائم وتعزيز الأمن المالي في العصر الرقمي:

١- تحديث التشريعات القانونية لمواكبة التطورات التكنولوجية.

- **اقتراح:** ضرورة تحديث الأنظمة القانونية الوطنية والدولية لمواكبة التطورات التقنية السريعة في مجال الجرائم الاقتصادية حيث يجب إدخال تشريعات واضحة تتعامل مع التحديات التي تفرضها التقنيات الحديثة مثل العملات الرقمية، والتعاملات عبر الانترنت، وتقنيات الذكاء الاصطناعي، والبلوكشين.

- **التنفيذ:** عقد ورش عمل تشريعية ودورات تدريبية للهيئات التشريعية لمواكبة آخر التطورات القانونية المتعلقة بالجرائم الاقتصادية الرقمية.

٢- تعزيز التعاون الدولي في مكافحة الجرائم الاقتصادية الرقمية.

- **اقتراح:** يجب تكثيف التعاون بين الدول في مجال تبادل المعلومات والبيانات المتعلقة بالجرائم الاقتصادية، خاصة تلك التي تحدث عبر الحدود، وإنشاء آليات مشتركة لرصد وتحليل المعاملات المالية المشتبه فيها، والتنسيق بين السلطات القضائية والتنظيمية.
- **التنفيذ:** تأسيس تحالفات دولية وشبكات اتصال بين هيئات مكافحة الجرائم المالية لتعزيز تبادل المعلومات بين السلطات الوطنية والدولية.

٣- تطوير استخدام الذكاء الاصطناعي في رصد الجرائم الاقتصادية.

- **اقتراح:** توظيف الذكاء الاصطناعي في تحليل البيانات الضخمة لرصد الأنماط المشبوهة في المعاملات المالية، مما يساهم في كشف الجرائم الاقتصادية بشكل أسرع وأكثر دقة، يمكن أن يساعد الذكاء الاصطناعي في تحديد التلاعبات المالية، وأنماط غسل الأموال، والاحتيال المالي.
- **التنفيذ:** تطوير حلول برمجية تعتمد على الذكاء الاصطناعي للكشف المبكر عن الجرائم الاقتصادية، وتنفيذ تلك الأنظمة بشكل مدمج مع الأنظمة المالية المستخدمة عالمياً.

٤- تعزيز التعليم والتوعية بأخطار الجرائم الاقتصادية.

- **اقتراح:** تعزيز برامج التعليم والتوعية على المستوى المجتمعي بشأن الجرائم الاقتصادية الرقمية وآثارها، وكيفية تجنب الوقوع في فخ الاحتيال الالكتروني. يمكن أن تشمل هذه البرامج المستهلكين، والموظفين في القطاع المالي، والمستثمرين، وكذلك الشركات الصغيرة والمتوسطة.
- **التنفيذ:** إطلاق حملات توعية عبر وسائل الاعلام ووسائل التواصل الاجتماعي، وتنظيم ورش عمل ومحاضرات حول الأمان الرقمي.

٥- تعزيز الشفافية والمساءلة في التعاملات المالية الرقمية.

- **اقتراح:** تبني تقنيات مثل البلوكشين لزيادة الشفافية في المعاملات المالية، وضمان تتبع الأموال وتوثيق العمليات المالية بشكل دائم وموثوق، بحيث يجب تشجيع البنوك والمؤسسات المالية على تبني هذه التقنيات في تعاملاتها.
- **التنفيذ:** تنظيم حملات توعية للبنوك والمؤسسات المالية حول مزايا تكنولوجيا البلوكين، وتقديم برامج دعم للتكامل مع أنظمة قائمة على هذه التكنولوجيا.

٦- تعزيز الرقابة والشفافية في منصات التجارة الالكترونية.

- **اقتراح:** ينبغي تكثيف الرقابة على منصات التجارة الالكترونية والأنشطة المالية المرتبطة بها، بما في ذلك عمليات الدفع عبر الانترنت، بحيث يجب أن تتمتع هذه المنصات بالقدرة على رصد المعاملات المشبوهة وتوثيقها بشكل فوري.
- **التنفيذ:** إلزام منصات التجارة الالكترونية بتطبيق معايير أمان صارمة، وتقديم تقارير دورية للسلطات المختصة حول الأنشطة المالية التي تجري عليها.

في نهاية الدراسة، وبهدف فتح آفاق جديدة نحو بحث آخر ينطلق مما توصلنا إليه في هذه الدراسة، نطرح الإشكالية التالية: مدى قدرة الدول والمجتمع الدولي في تطوير آليات قانونية وتكنولوجية فعالة لمكافحة الجرائم الاقتصادية العابرة للحدود، في ظل مواكبة الفاعلون غير الدول لكل التطورات التكنولوجية المتسارعة مع ما يستتبع ذلك من تأثيرات على التنمية المستدامة خاصة في الدول النامية.

المصادر والمراجع.

- **القرآن الكريم.**

1- Council of Europe. Convention on Cybercrime (ETS No. 185). Strasbourg: Council of Europe, 2001, www.coe.int/ date of visit 3/3/2025.
2- Cyber Security in Canada Addressing the Growing Threat of Cybercrime". (2018). The Globe and Mail, www.theglobeandmail.com, date of visit, 25/1/2025.
3- Fico. (2020). Fico Falcon Fraud Management: protecting business and consumers from financial fraud. Fico. San Jose, CA, USA, www.fico.com. Date of visit 4/3/2025.
4- Financial Action Task Force (FATF). 2012, The FATF Recommendations, Paris, France, 2012.
5- Glaeser, Edward L., Sacerdote, Bruce. (2000). The Economic Approach to crime, Published by Elsevir, United States.
6- Hern, A. (2014). "Sony Hack: How the Cyberattack Unfolded", www.theguardian.com, / technology/2014/dec/17/sony-hack-cyberattack-unfolded, date of visit to the website, 1/3/2025.
7- Interpol. (2014). Operating Sky Net: Coordinated international effort to Combat cybercrime. Lyon, France. www.interpol.int. date of visit, 7/3/2025.
8- Interpol. (2018). Operating Emerald: Global Action Against the illicit Trafficking of Wildlife. Lyon: Interpol, 2018. www.interpol.int. date of visit 7/3/2025.
9- Kharouf, Omar M. (2020). "Digital Banking: Strategies for launching or Becoming a Digital Bank". Palgrave Macmillian, 2020.
10- Laudon, Kenneth C., and Carol Guercio Traver. E-commerce: Business, Technology, Society. 15th ed. Pearson, 2021, Boston, MA
11- Levi, M. (2008). Organized Crime and the politics of Crime Control. In the Oxford Handbook of Criminology (4th ed.).