دراسات خاصة

سلسلة دراسات غير دورية تصدر عن المستقبل للأبحاث والدراسات المتقدمة أبوظبي، الإمارات العربية المتحدة

الصناعة والمكافحة:
كيف يُغير الذكاء الاصطناعي مشهد الجريمة الاقتصادية؟

إعداد: د. رشا مصطفى عوض

العدد 29 - يوليو 2024

دراسات خاصة

عن "دراسات خاصة"

سلسلة دراسات غير دورية تصدر عن "المستقبل للأبحاث والدراسات المتقدمة"، وتركز الدراسات على الظواهر الصاعدة، والمؤشرات المركبة والأفكار غير التقليدية، والاتجاهات القادمة التي ترتبط بالعالم قيد التشكل منذ بداية عام 2020.

وتتناول "السلسلة" أبرز القضايا الصاعدة في المجالات الأمنية والسياسية والاقتصادية والاجتماعية والتكنولوجية، والظواهر كافة التي يمكن أن تساهم في تشكيل مستقبل التفاعلات الدولية والإقليمية.

الصناعة والمكافحة:

كيف يُغير الذكاء الاصطناعي مشهد الجريمة الاقتصادية؟

د. رشا مصطفى عوض

خبير اقتصادي ومستشار رئيس المركز للسياسات العامة، مركز المعلومات ودعم اتخاذ القرار – مجلس الوزراء المصري

مقدمة الدراسة:

ثمة لحظات تقنية تصنع تحوُّلات جوهرية في تاريخ البشرية؛ إنها تلك اللحظات التي تؤرخ لإطلاق أو اكتشاف تقنيات مُبتكرة، أو بدء انتشارها واستخدامها واسع المدى؛ الأمر الذي ينعكس لدرجة هائلة على الصناعات والمجتمعات فتغيِّر العالم بأسره. من بين اللحظات التقنية الفائتة اختراع يوهانس غوتنبرغ آلة الطباعة في عام 1455، وظهور أول حاسب آلي شخصي عام 1974. وعلى ذات المِنوال، تصف كتابات عدة عام 2023 بأنه "لحظة الذكاء الاصطناعي".

بينما يُتابع العالم عن كثب الاستخدام المُتنامي للتقنيات والتطبيقات المؤيدة بالذكاء الاصطناعي، يُشير ساندر بيتشاي، الرئيس التنفيذي لشركة "جوجل" الأمريكية إلى "أننا نقف على عتبة لحظة الذكاء الاصطناعي، الذي سيُحدث ثورة في جميع مناحي الحياة". إنها نقطة التحوُّل المحورية التي تصف التقدم المُتسارع والانتشار المُتنامي لتقنيات الذكاء الاصطناعي، لتُعيد هيكلة اقتصادات البلدان، وتُغيِّر نمط العلاقة بين الإنسان والتكنولوجيا. بيد أن هذه المكاسب اللامحدودة يواجهها على طرف نقيض مزيد من المساحات القابلة لنشوء الجريمة الاقتصادية فتُصبح أكثر تطوراً وخطورة.

لقد أضحى للذكاء الاصطناعي دور رئيس في اتساع نطاق الجريمة السيبرانية ودرجة تعقدها، حتى إن تقديرات حديثة تتوقع ارتفاع تكلفتها عالمياً لتُسجل 20 تريليون دولار أمريكي بحلول عام 2026، بعد أن بلغت 6 تريليونات دولار في 2021؛ يواكب ذلك أيضاً بزوغ عهد جديد لجرائم الاحتيال المؤيدة بتقنيات الذكاء الاصطناعي؛ إذ يُنذرنا سيدارت فينكاتارا ماكريشنان، في مقاله بصحيفة "فايننشال تايمز" البريطانية منشورة في 19 يناير 2024، بأن "الذكاء الاصطناعي يُبشر بالجيل القادم من عمليات الاحتيال المالي".

وبالتوازي، تطورت جريمة "غسل الأموال"، التي تتراوح تكلفتها السنوية ما بين 1.4 و3.5 تريليون دولار، والتي صارت مؤيدة بالذكاء الاصطناعي؛ لأنه يُسهم في تسهيل عملية إخفاء الأصول المالية غير المشروعة، وتمويه طبيعة المعاملات لتجنب اكتشافها من قِبل السلطات التنظيمية والقانونية. اللافت للانتباه أن دينامية الساحة الدولية للجريمة الاقتصادية المؤيدة بالذكاء الاصطناعي لا تقتصر على هذه الجرائم الثلاث فقط –الجريمة السيبرانية والاحتيال وغسل الأموال– ولكنها تمتد لغالبية فئاتها الأخرى.

وهكـذا، يشـهد العالـم سـباقاً محمومـاً للتسـلح بتقنيـات الـذكاء الاصطناعـي، عـبر عنـه فاتسـا ناراسـيمها، الرئيـس التنفيـذي لشركـة "كومبـلاي أدفانتـج" البريطانيـة (ComplyAdvantage) في مطلـع عـام 2024 قائـلاً: "لقـد أضحـى الـذكاء الاصطناعـي أداة لـكل مـن المُجرمـين والمؤسسـات؛ إذ يسـتخدمه المُجرمـون لابتـكار أسـاليب جديـدة للاحتيـال عـلى العُمـلاء، بينمـا تسـتفيد منـه المؤسسـات للتغلـب عـلى المُحتالـين وحماية عملائهـا". ولعـل ذلـك يطـرح تسـاؤلاً حـول طبيعـة هـذا السِّـجال، والمقومـات التـي يُمكـن أن تُعـين الفريـق الأخـير للتفـوق عـلى الأول. تلـك هـي الإشـكالية التـي تطرحهـا هـذه الدراسـة مُسـتندة إلى منهـج التحليـل الاسـتقرائي ومراجعـة الأدبيـات والكتابـات السـابقة، مـع إشـارة خاصـة لعـدد مـن النمـاذج ودراسـات الحالـة.

جـاءت الدراسـة في سـتة أقسـام؛ اختـص القسـم الأول منهـا بتبيـان ماهيـة الجريمـة الاقتصاديـة المُؤيـدة بالـذكاء الاصطناعـي، واسـتعرض القسـم الثانـي المشـهد الراهـن لهـا وتداعياتهـا الرئيسـة. ثـم ألقـى القسـم الثالـث الضـوء عـلى جريمـة الاحتيـال المـالي المؤيـدة بالـذكاء الاصطناعـي كدراسـة حالـة. وانتقـل القسـم الرابـع إلى مناقشـة دور الـذكاء الاصطناعـي في مكافحـة الاحتيـال المـالي، في حـين ألقـى القسـم الخامـس الضـوء عـلى عـدد مـن التحديـات والفـرص المسـتقبلية لمكافحـة الجريمـة الاقتصاديـة. وأخـيراً، قدَّمـت الدراسـة بعـض الملاحظـات الختاميـة في القسـم السـادس.

أولاً: ماهية الجريمة الاقتصادية المؤيدة بالذكاء الاصطناعي

في عالـم الجريمـة ديناميكـي التطـور، تُعـدُ الجريمـة الاقتصاديـة مُكوِّنـاً رئيسـاً تحـت مظلـة "الجريمـة المُنظمـة"، التـي يعرفهـا "مكتـب الأمـم المتحـدة المعنـي بالجريمـة والمُخـدرات" بأنهـا "ظاهـرة دائمـة التحـول تمسُّ جميـع البلـدان، تقـوم بهـا جماعـات مُنظمـة تضـم ثلاثـة أشـخاص أو أكثـر، وتتسـم بقـدر مـن التنظيم الهيـكلي، ويمتـد وجودهـا فـترةً مـن الزمـن، وتهـدف إلى ارتـكاب واحـدة عـلى الأقـل مـن الجرائـم الخطـرة للحصـول عـلى منفعـة ماليـة أو ماديـة أخـرى". ولا غـرو أن تقنيـات الـذكاء الاصطناعـي قـد عقـدت الجريمـة الاقتصاديـة بشـكل أكـبر.

1. تعريـف الجريمـة الاقتصاديـة وفئاتهـا الرئيسـة: عنـد البحـث في أصـول مصطلـح الجريمـة الاقتصاديـة، سـوف نجـد أن عالـم الاجتمـاع والجريمـة إدويـن سـاذرلاند قـد صـك أواخـر ثلاثينيـات القـرن العشريـن مصطلـح "جرائـم ذوي الياقـات البيضـاء"، الـذي جـاء عـلى نقيـض "جرائـم ذوي الياقـات الزرقـاء"، والتـي تختلـف أيضـاً عـن "جرائـم الشـارع". في حـين ترتبـط "جرائـم الشـارع" باسـتخدام أسـلحة وعُنـف مثـل: القتـل والسرقـة والسـطو المُسـلح، تنطـوي الفئـة الأولى عـلى جرائـم يرتكبهـا "أنـاس مسـؤولون في مناصبهـم الوظيفيـة"، يرتـدون عـادة قمصانـاً ذات أزرار وياقـات بيضـاء، ويتمتعـون بمكانـة اجتماعيـة مرموقة ومسـتوى تعليمـي مرتفـع.

ورغـم أن "جرائـم ذوي الياقـات البيضـاء" لا تنطـوي عـادة عـلى قـدر مـن العنـف الجسـدي، فإنهـا تتسـبب في خسـائر ماليـة كبـيرة مُبـاشرة وغـير مُبـاشرة. ولضمـان توحيـد الأنمـاط المختلفـة لمثـل هـذه الجرائـم تحـت مظلـة واحـدة، وضعـت "إدارة العـدل الأمريكيـة" في عـام 1981 تعريفـاً آخـر لـ "جرائـم ذوي الياقـات البيضـاء"، بوصفهـا جريمـة غـير عنيفـة لتحقيـق مكاسـب ماليـة عـن طريـق الخِـداع، يرتكبهـا شـخص مـا لديـه معرفـة فنيـة ومهنيـة خاصـة بالأعمـال التجاريـة والحكوميـة، أيـاً كانـت المهنـة التـي يُمارسـها. في حـين وصفهـا هـيرب إدلهيرتـز بـ "**الجريمـة الاقتصاديـة**"، وعرَّفهـا بأنهـا فعـل أو سلسـلة مـن الأفعـال التـي يتم

ارتكابها بأساليب غير مادية، بالخداع والتزييف للحصول على أموال أو ممتلكات، أو تجنب دفع أموال أو التخلي عن ممتلكات أو خسارتها، أو للحصول على مزايا تجارية أو شخصية غير مُستحقة.

اتصالاً، طرح إدلهيرتز نظاماً لتصنيف الجرائم الاقتصادية وفقاً لطبيعة مُرتكبيها، وإن كانت تشترك جميعها في نية ارتكاب فعل غير مشروع لتحقيق أغراض ومكاسب غير قانونية، ويضم النظام أربع فئات رئيسة كالتالي:

- جرائم يرتكبها أشخاص يعملون فُرادى وفق نهج غير مُنتظم؛ مثل: التهرب الضريبي، والاحتيال باستخدام البطاقات الائتمانية المصرفية.
- جرائم يرتكبها أشخاص أثناء تأدية مهامهم الوظيفية سواء حكومية أم غير حكومية، ينتهكون بموجبها ولاءهم لجهة العمل، ومن أمثلتها تقاضي الرشاوى والعمولات.
- جرائم تقوم بها مؤسسات لتحقيق مكاسب غير مشروعة، وتخص أنشطة مُساندة لعملياتها التجارية الأصيلة، ومنها على سبيل المثال، انتهاك أكواد البناء أو الاعتبارات البيئية.
- جرائم يرتكبها "ذوو الياقات البيضاء" تمس عملاً تجارياً أو نشاطاً اقتصادياً أصيلاً، مثل: جرائم الاحتيال المالي والتجاري والتأميني.

وفي سياق مُتصل، يُمكن تصنيف الجريمة الاقتصادية وفقاً لطبيعة الفعل المُرتكَب، والمُقترح أن تضم اثنتي عشرة فئة كما يعرضها الجدول رقم (1). جدير بالذكر أنه لا يوجد تصنيف وحيد مُتعارف عليه، لذلك استند الباحث في طرحه إلى عدد من التصنيفات الرئيسة، منها هيكل الاتحاد الأوروبي لتقدير مخاطر الجريمة المُنظمة والخطرة (EU Serious and Organized Crime Threat Assessment). كما تم اشتقاق مُصطلح "الجريمة المالية" باعتبارها مجموعة فرعية من "الجريمة الاقتصادية"، والتي ترتبط في الأساس بأنظمة أو مؤسسات أو أدوات مالية؛ مثل: غسل الأموال والاحتيال المالي.

جدول (1). تصنيف الجريمة الاقتصادية وفقاً لطبيعتها

الفئة	التصنيف الفرعي
الجرائم السيبرانية	▪ الهجمات السيبرانية ▪ انتهاكات البيانات ▪ برامج الفدية ▪ سرقة الهوية ▪ الاستغلال الجنسي للأطفال عبر الإنترنت ▪ الاحتيال في المدفوعات غير النقدية

الفئة	التصنيف الفرعي
التلاعب المالي	▪ التلاعب بالأسواق ▪ التداول من الداخل ▪ الاحتيال في الأوراق المالية
تزوير العملة	▪ تزييف العملة
تمويل الإرهاب	▪ تمويل الأنشطة والجماعات الإرهابية
غسل الأموال	▪ المعاملات المالية غير القانونية بهدف إخفاء مصدر الأموال التي تأتي عادة من أنشطة غير مشروعة
الاحتيال	▪ الاحتيال الاستثماري ▪ الاحتيال المصرفي ▪ الاحتيال الرومانسي ▪ احتيال الرئيس التنفيذي ▪ الاحتيال بشأن الاستيراد الجمركي ▪ الاحتيال بشأن المزايا الاجتماعية ▪ الاحتيال بشأن الإعانات ▪ الاحتيال الضريبي ▪ الاحتيال المستندي ▪ الاحتيال عبر اختراق البريد الإلكتروني الخاص بالأعمال التجارية ▪ الاحتيال في عدم التسليم ▪ الاحتيال على المستهلك / المبيعات الاحتيالية ▪ الإعلانات الكاذبة ▪ الممارسات التسويقية الخادعة

الفئة	التصنيف الفرعي
الفساد والرشوة	▪ الفساد والرشوة ▪ إساءة استخدام المعلومات السرية أو الإفصاح عنها لأشخاص غير مُصرح لهم
تزييف المُنتجات	▪ تزييف السلع ▪ الاحتيال في الأطعمة والمشروبات ▪ الجرائم الصيدلانية ▪ قرصنة المحتوى الرقمي
الاقتصاد غير الرسمي	▪ الأنشطة الاقتصادية غير الرسمية
سرقة الملكية الفكرية	▪ انتهاك حقوق الطبع والنشر ▪ انتهاك براءات الاختراع ▪ انتهاك العلامات التجارية ▪ قرصنة التصميم
الإنسان كسلعة	▪ تهريب المُهاجرين ▪ الاتجار بالبشر ▪ الاستغلال الجنسي ▪ الاستغلال في العمل ▪ الاتجار بالأطفال
الجرائم البيئية	▪ جرائم النفايات والتلوث ▪ جرائم الحياة البرية ▪ جرائم الغسل الأخضر

المصدر: قام الباحث بتطوير المحتوى وفقاً لعدد من الأدبيات والتقارير ذات الصلة.

2. جرائم اقتصادية مؤيدة بالذكاء الاصطناعي: تُضيف التقنيات الناشئة تحديات مُتجددة إلى ساحة الجريمة الاقتصادية؛ إذ يستفيد منها المجرمون لشن هجمات متطورة، أو إحباط تكنولوجيات مُصممة للكشف عنهم. ولا شك في أن قدرات "الذكاء الاصطناعي التوليدي" (Generative Artificial Intelligence) تُتيح آفاقاً جديدة لهذا النوع من الجرائم؛ إذ أكد 66% من بين 600 متخصص في مجال الامتثال للخدمات المصرفية والمالية -خلال مقابلات أجرتها شركة "كومبلاي أدفانتج"- أن استخدام المُحتالين للذكاء الاصطناعي يزيد من درجة تعقد الهجمات السيبرانية ونطاقها.

كما يخلص تقرير "سومسوب السنوي للاحتيال في مجال الهوية" (Sumsub Identity Fraud Report) لعام 2023 إلى أن "الاحتيال المدعوم بالذكاء الاصطناعي" يُعد الجريمة الأكثر خطورة عالمياً في الوقت الحاضر؛ ليتقدم بذلك على جرائم عتيدة مثل: شبكات تهريب الأموال والهويات الشخصية المُزورة، والاستيلاء على الحسابات المصرفية. اللافت للانتباه أن جرائم الاحتيال تضم أنواعاً غاية في الخطورة، يأتي في مقدمتها ثلاثة رئيسيون.

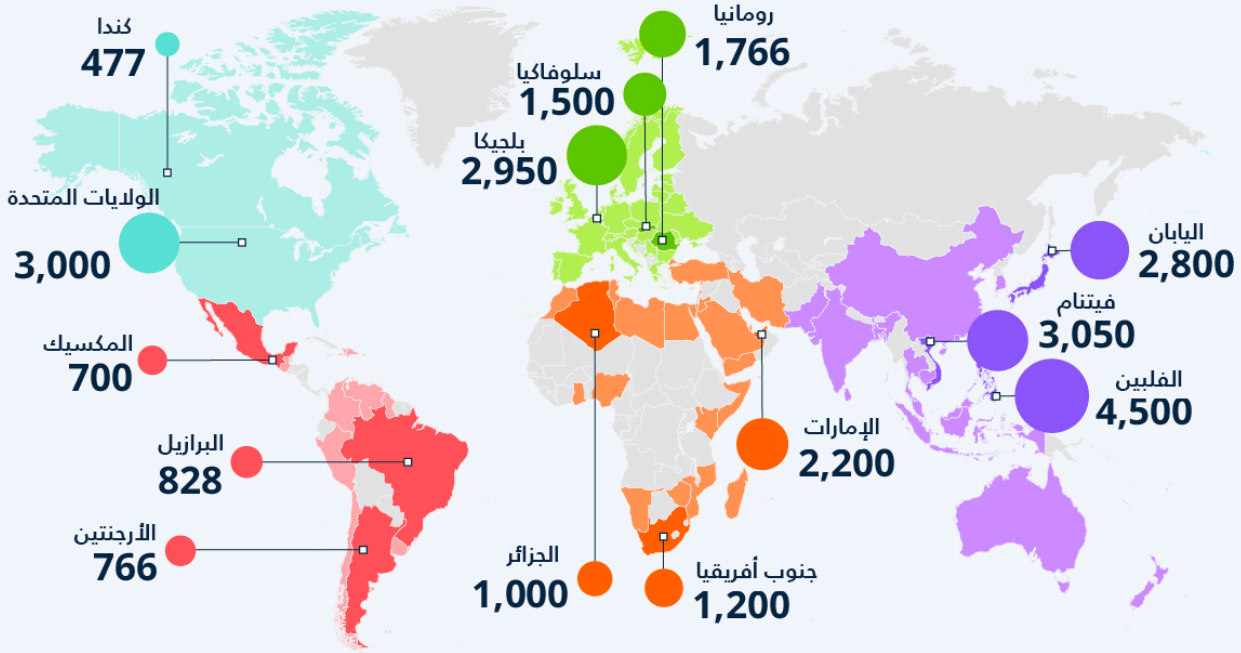
تتمثل الجريمة الأولى في "التزييف العميق" الذي يستخدم الذكاء الاصطناعي التوليدي لإنتاج مُحتوى اصطناعي مُقنِع لأناس يقولون أو يفعلون أموراً وهمية وغير حقيقية، سواء أكان في هيئة صور أم مقاطع فيديو أم مقاطع صوتية. كما تُستخدم هذه التقنية لإنشاء شخصيات غير واقعية لا وجود لها في العالم الفعلي. لذلك، يصفها البعض بأنها أخطر تهديد مجتمعي، خاصة وأن الكشف عن المُحتوى المُزيَّف تشوبه صعوبات عدة. ووفقاً لتقرير "سومسوب"، ارتفع عدد حالات التزييف العميق المُعلن عنها خلال عام 2023 بنحو عشرة أمثال ما كانت عليه في عام 2022، وسجلت الفلبين أكبر مُعدل زيادة بواقع 4500% كما يُوضح الشكل (1).

يختص النوع الثاني بجرائم "التصيد الاحتيالي المدعوم بالذكاء الاصطناعي" (AI-powered Phishing)، التي يُطلق عليها أيضاً مصطلح "التصيد العميق"؛ لأنها تتبع أسلوباً جديداً للتصيُّد باستخدام مزيج من تقنية "التزييف العميق" وأساليب "الهندسة الاجتماعية" (Social Engineering)، وتُشير الأخيرة إلى مجموعة كبيرة من الأنشطة الضارة التي يقوم بها مرتكب الجريمة خلال تفاعله مع الضحايا للتلاعب بهم نفسياً، واستغلال ثقتهم لتجاوز الإجراءات الأمنية التقليدية؛ ما يقود الضحايا للكشف عن معلوماتهم السرية أو إتاحة الوصول إلى موارد حيوية مُصرح لهم بالنفاذ إليها، مثل: النظم الإلكترونية وحسابات البريد الإلكتروني، أو حتى تنفيذ معاملات مصرفية؛ ومن بين أدوات المُهاجمين في هذا السياق:

- **رسائل البريد الإلكتروني أو الرسائل النصية:** ومن أمثلتها هجمات "الاحتيال عبر اختراق البريد الإلكتروني الخاص بالأعمال التجارية" أو "احتيال الرئيس التنفيذي"، الذي يعرف بانتحال صفة مسؤولين تنفيذيين رفيعي المستوى؛ وما يزيد من خطورة هذه الجرائم أن المُحتالين يستخدمون تقنية التزييف العميق لجعل الرسائل أكثر خصوصية، فتبدو هوياتهم المُزيفة أكثر مصداقية.
- **مُكالمات الفيديو والرسائل الصوتية:** يتم تزييف هذه الملفات باستخدام تقنيات التزييف العميق التي تزيد من الحبكة الخداعية؛ لتتم مشاركتها مع الضحايا لاستغلالهم. مثال على ذلك، كشفت شرطة هونغ كونغ في فبراير 2024 عن خِداع موظف بالإدارة المالية لشركة متعددة الجنسية عبر

تزييف اجتماع افتراضي جماعي بحضور المدير المالي للشركة -المُنتحل صفته- ليطالب الأخير بتحويل مبلغ 25 مليون دولار للمُحتالين، فيُنفذ الأمر في لحظتها، ولا يزال مرتكبو الجريمة مجهولي الهوية.

شكل (1): الدول ذات معدل الزيادة الأكبر في حالات الاحتيال المرتبطة بالتزييف العميق في عام 2023 مقارنة بعام 2022 (معدل التغير السنوي %) *



* تستند البيانات المُوضحة إلى النتائج الصادرة ضمن تقرير "سومسوب السنوي للاحتيال في مجال الهوية 2023"، الذي اعتمد على تحليل أكثر من 2 مليون حالة احتيال في الهوية من 224 دولة وولاية.

Source: Zandt, F. (2024, March 13). How Dangerous are Deepfakes and Other AI-Powered Fraud? Statista. https://tinyurl.com/3nwm5tra

وأخيراً، يرتبط النوع الثالث بجرائم "الاحتيال عبر البيانات الاصطناعية" (Synthetic Data Fraud) بإنشاء بيانات مُصطنعة أو التلاعب بها لخداع أفراد أو مُنظمات. مثال على ذلك، أعلنت شركة "إكويفاكس" (Equifax) –وهي واحدة من أكبر ثلاث وكالات للاستعلام الائتماني الاستهلاكي في الولايات المتحدة الأمريكية– في سبتمبر 2017 عن تعرضها لاختراق أمني سيبراني؛ إذ قام مرتكبو الجريمة بالنفاذ إلى بيانات ما يزيد على 147 مليون فرد من عملائها، بما في ذلك تواريخ الميلاد وأرقام حسابات الضمان الاجتماعي وأماكن إقامتهم وحالتهم الائتمانية، وتم استخدام هذه البيانات لإنشاء هويات مُصطنعة عن طريق المزج بين معلومات حقيقية وأخرى وهمية، بدلاً من انتحال شخصية شخص حقيقي؛ ليتم استخدامها في أنشطة احتيالية أخرى.

وبطبيعة الحال، يصبح من الصعب اكتشاف هذا النوع من الاحتيال؛ لأنه لا يرتبط بعملية سرقة لهويات حقيقية يتم الإبلاغ عن فقدها. جدير بالذكر أن دراسة حديثة قد خلصت إلى أن الاحتيال باستخدام الهوية الاصطناعية تسبب في خسارة المؤسسات المالية لنحو 20 مليار دولار في عام 2020. كما أشار تقرير آخر إلى أن مؤسسات الإقراض عبر الإنترنت تخسر حوالي 6 مليارات دولار سنوياً بسبب هذا النوع من الاحتيال.

ثانياً: المشهد الراهن للجريمة الاقتصادية وتداعياتها

تُسهم عوامل عدة في الواقع المُتنامي للجريمة الاقتصادية، يأتي في مقدمتها التقدم التقني، وجائحة "كورونا" التي غيَّرت كثيراً من أنماط الحياة، وتطور الأنظمة المالية الراهنة، وتعقد البيئة الجيواقتصادية، والعوامل الاقتصادية والاجتماعية، وغير ذلك من عوامل. ولا عجب أن ذلك واكبه تعاظم التكاليف المُباشرة التي يتحملها المُجتمع العالمي جراء هذه الجرائم، التي تُقدر بعدة تريليونات من الدولارات الأمريكية، مع تصاعد تكلفتها بمرور الوقت.

1. واقع الجريمة الاقتصادية: يُغذي الاستخدام غير المشروع للتقنيات التكنولوجية المُتقدمة مشهد الجريمة الاقتصادية. فلقد أصبحت الجرائم الإلكترونية أكثر انتشاراً مع استغلال المجرمين لنقاط الضعف في الأنظمة الإلكترونية والشبكات الرقمية ذات الانتشار المُتنامي. كذلك فإن ترابط الأسواق العالمية (مثل التجارة الإلكترونية) وتعقد الأنظمة المالية (مثل أنظمة الدفع الإلكتروني) التي تتجاوز حدود الدولة الوطنية عابرة القومية، وظهور الابتكار المالي والتكنولوجيا المالية والعُملات الرقمية قد أسهم في اتساع نطاق الجريمة الاقتصادية وأضفى صعوبة على تعقبها واكتشافها ومُحاسبة مُرتكبيها.

وتزيد التطورات المتلاحقة في النظام الجيواقتصادي الدولي والتوترات الجيوسياسية من الجريمة الاقتصادية. إنها تخلق فرصاً جديدة للاحتيال وغسل الأموال والهجمات السيبرانية؛ إذ يقوم المُجرمون بمواءمة استراتيجياتهم لاستغلال ثغرات في البنية التحتية الرقمية والنظام البيئي الاقتصادي. كذلك، قد تدفع الأزمات والصعوبات الاقتصادية والاجتماعية (مثل البطالة والفقر) مزيداً من الأفراد والجماعات لارتكاب مثل هذه الجرائم.

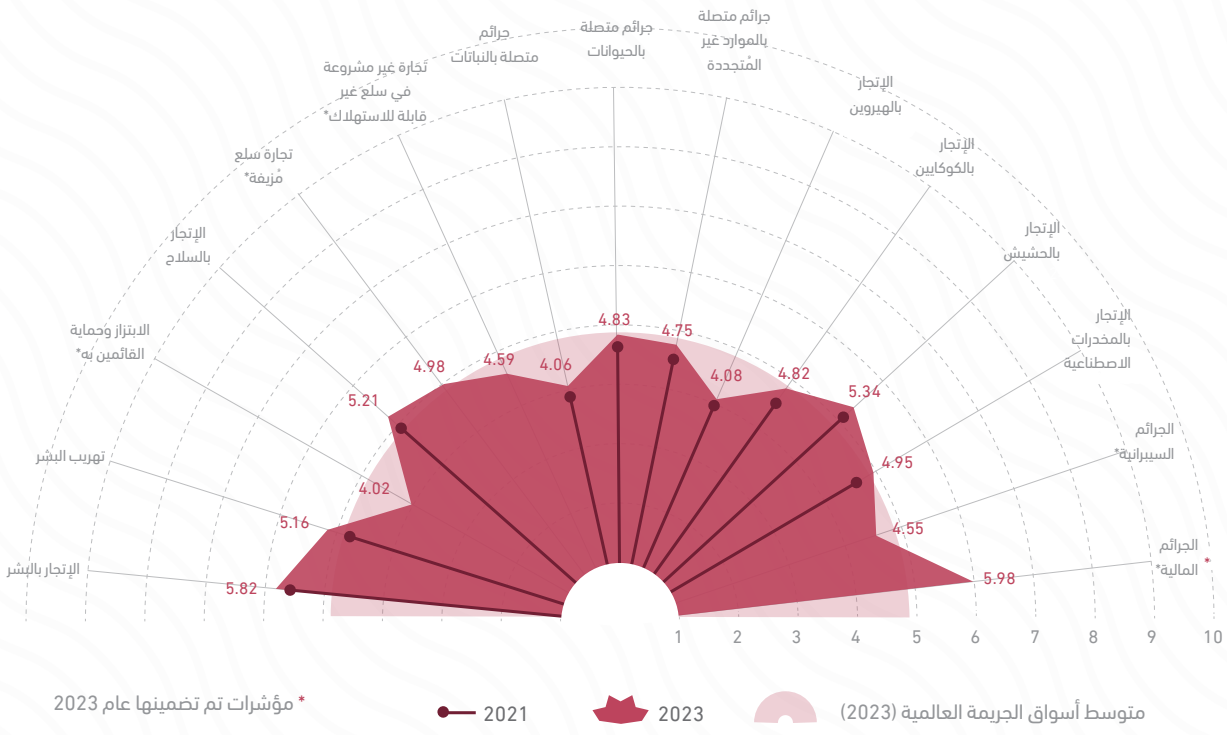
أيضاً، تؤثر الأوبئة في مشهد الجريمة الاقتصادية. وفي هذا السياق، خلصت ورقة سياسات صادرة في سبتمبر 2020 عن "وحدة خدمة بحوث الكونغرس الأمريكي" (Congressional Research Service) إلى أن جائحة "كورونا" أفرزت مخاطر جديدة مُتصلة بالجرائم الإلكترونية؛ إذ:

- ساعدت عمليات الحجر الصحي الطوعية على زيادة وتيرة التعاملات المصرفية الإلكترونية، مما شكَّل تحدياً للمؤسسات المالية بشأن الامتثال لمتطلبات مكافحة غسل الأموال وتمويل الإرهاب.
- دفعت التقلبات المالية خلال فترة الجائحة بعض المستثمرين إلى إعادة هيكلة محافظهم المالية، مع زيادة نسبة الممتلكات النقدية المادية، وأصول الملاذ الآمن (مثل الذهب) والعقارات؛ ما نتج عنه تحوُّل العالم تجاه اقتناء أصول مادية أقل شفافية وأكثر صعوبة في التتبع.

- زادت حوادث التداول من الداخل (Inside Trading)؛ إذ استفاد أناس كُثر من المعلومات السرية غير المُفصح عنها، والمتعلقة بتأثير جائحة "كورونا" في الأسواق المالية. كما انتشرت جرائم التلاعب بالسوق لاستغلال التقلبات في أسعار الأسهم والسلع.

في هذا السياق، تُشير نتائج "مؤشر الجريمة المنظمة العالمية لعام 2023" الصادر عن "المبادرة العالمية لمكافحة الجريمة المُنظمة عابرة القومية" (Global Initiative Against Transnational Organized Crime) المُوضحة بالشكل رقم (2) إلى أن الجرائم المالية -التي تم إدراجها للمرة الأولى ضمن تقرير عام 2023– كانت الأكثر انتشاراً بين جميع أنواع الجرائم الأخرى، مُسجلة 5.98 درجة من إجمالي 10 درجات، حتى إنها تقدمت على جريمة الاتجار بالبشر التي احتلت المركز الأول لسنوات، وإن كان ذلك لا يعني انخفاض خطورة الأخيرة؛ إذ تُظهر النتائج ارتفاع قيمة مؤشرها خلال الفترة (2021 – 2023).

شكل (2): مؤشر أسواق الجريمة: المتوسطات العالمية عام 2023 مقارنة بعام 2021



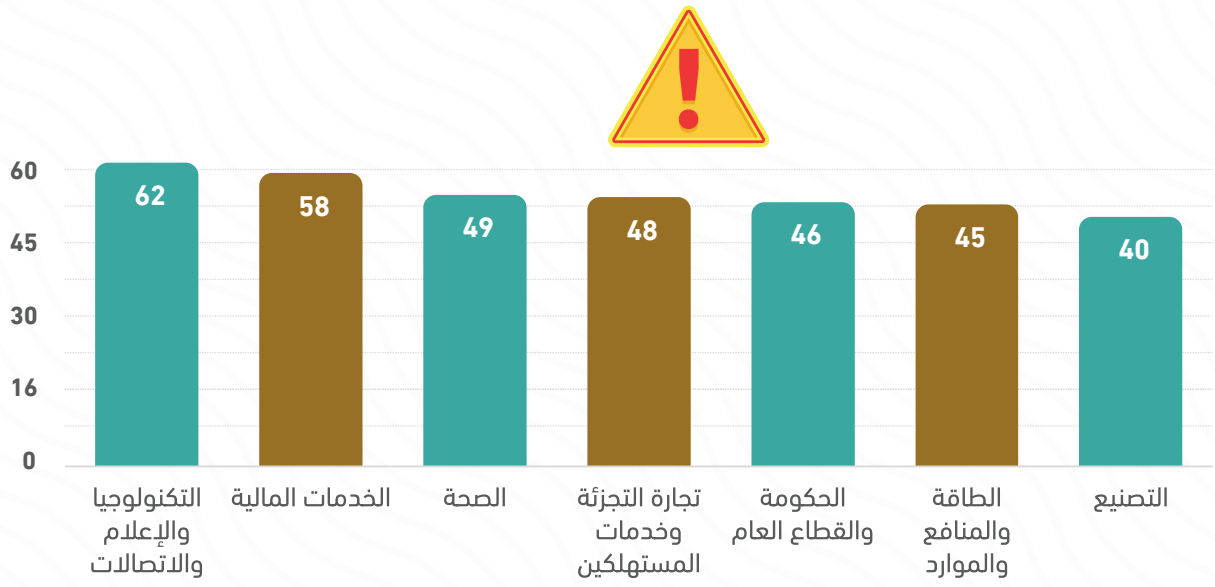
Source: Global Initiative Against Transnational Organized Crime. (2023). Global Organized Crime Index 2023. Geneva. https://tinyurl.com/4yjet5e7

اللافت للانتباه أن جرائم اقتصادية أخرى جاءت في مرتبة متقدمة وفقاً لنتائج المؤشر؛ منها جرائم الاتجار بسلع مُزيفة، والتجارة غير المشروعة في سلع غير قابلة للاستهلاك والجرائم السيبرانية، مُسجلة 4.98 و4.59 و4.55 درجات على التوالي. أيضاً، خلصت نتائج المؤشر إلى أن 133 دولة قد عانت بشدة من الجريمة الاقتصادية وتبعاتها؛ أي ما يقرب من 70% من الدول الأعضاء في الأمم المتحدة؛ الأمر الذي يعكس تحولها إلى ظاهرة عالمية، وتزايد قدرتها على تقويض الهياكل الاجتماعية والاقتصادية.

ووفقاً لنتائج مسح "الجريمة الاقتصادية والاحتيال لعام 2022" (Global Economic Crime and Fraud Survey) الصادر عن شركة "برايس ووتر هاوس كوبرز" (Price Waterhouse Coopers)، ذكر 46% من المشاركين في المسح (بإجمالي 1296 مديراً تنفيذياً عبر 53 دولة) أن مؤسساتهم تعرضت لجريمة اقتصادية واحدة على الأقل خلال العامين السابقين على إجرائه. وفيما يخص الفئات الأكثر تأثراً بهذه الحوادث، فكانت كالتالي:

- المؤسسات العاملة في قطاع التكنولوجيا والإعلام والاتصالات، تليها المؤسسات المالية بنحو 62% و58% من الإجمالي على التوالي، كما يوضح الشكل رقم (3).
- مؤسسات الأعمال الأكبر حجماً التي تزيد إيراداتها السنوية عن 10 مليارات دولار بنسبة 52% من إجمالي الفئة، في حين شهدت 38% من المؤسسات التي تقل إيراداتها السنوية عن 100 مليون دولار جرائم اقتصادية واحتيالاً.

شكل (3): مسح الجريمة الاقتصادية والاحتيال لعام 2022: نسبة الإبلاغ عن جريمة اقتصادية واحدة على الأقل خلال العامين السابقين على المسح (% من إجمالي المشاركين وفقاً للنشاط الاقتصادي)



Source: PwC. (2023). PwC's Global Economic Crime and Fraud Survey 2022. https://tinyurl.com/bdukdmut

2. تداعيات الجريمة الاقتصادية: تتعدد الآثار والتداعيات المباشرة وغير المباشرة الناتجة عن الجريمة الاقتصادية، والتي يأتي في مقدمتها الخسائر المالية. فقد كشف عن ذلك 53% من إجمالي المُشاركين في مسح الجريمة الاقتصادية والاحتيال لعام 2022، لتأتي بذلك في مقدمة الآثار الناتجة عن هذه الجرائم، والتي تتعاظم تكلفتها في أحيان كثيرة. فعلى مستوى مؤسسات الأعمال الأكبر حجماً التي شملها المسح (ذات إيرادات سنوية بقيمة 10 مليارات دولار فأكثر) والتي تعرضت لجرائم اقتصادية واحتيال، تكبدت 18% منها خسارة مالية تزيد على 50 مليون دولار، في حين ذكرت 22% من مؤسسات الأعمال صغيرة الحجم أن الجريمة الأكثر إيلاماً كلفتها ما لا يقل عن مليون دولار.

أيضاً، تتسبب جرائم التلاعب بالأسواق والتعاملات المالية غير المشروعة والتداول من الداخل وجرائم اقتصادية أخرى في إحداث تشوهات سوقية لتأثيرها في ديناميكيات العرض والطلب؛ ومن ثم الأسعار؛ الأمر الذي يُقوض سلامة الأسواق. وقد يتخطى حدود السوق المُتأثرة مباشرة نتيجة اتساع آثارها الانتشارية وترابط الأسواق العالمية. مثال على ذلك، أظهر صندوق النقد الدولي أن قصور عمليات مكافحة غسل الأموال وتمويل الإرهاب في منطقة بحر البلطيق الشمالي قد نتج عنه حدوث انخفاضات كبيرة في أسعار أسهم البنوك المتأثرة بشكل مباشر، وكذلك أسعار أسهم البنوك الأخرى العاملة في نفس البلد، وفي الإقليم الجغرافي المُتصل به.

إضافة إلى ما تقدم، تُعوق الجريمة الاقتصادية الجهود الوطنية للنمو والازدهار الاقتصادي؛ لأنها تؤدي إلى خسائر مالية جمة وتحويل الموارد بعيداً عن الأنشطة الإنتاجية الرسمية، مع خفض الإيرادات الحكومية. وقد تقود هذه الجرائم إلى خفض معدلات التوظيف؛ إذ تلجأ بعض مؤسسات الأعمال لخفض العمالة بعد تكبدها خسائر مالية جراء عمليات احتيال مالي. هذا بالإضافة إلى فقدان الثقة في مؤسسات الدولة –خاصة المؤسسات المالية والهيئات التنظيمية ذات الصلة– مما ينعكس سلباً على تدفقات الاستثمار ويُضعف القدرات الشاملة لاقتصادات الدول وتنافسيتها إقليمياً وعالمياً.

اتصالاً بذلك، هناك تداعيات اجتماعية وإنسانية للجريمة الاقتصادية على الأفراد والمجتمعات؛ إذ تؤثر هذه الجرائم في مستوى الأمن والرفاه الإنساني، وقد تخلق حالة من الخوف والمعاناة بين أفراد المجتمع؛ لأنها تؤدي إلى تأثيرات عدة تأتي في مقدمتها:

- صعوبات مالية جراء فقدان أموال أو استثمارات أو أصول؛ مما يضر بالمستوى المعيشي للضحية وأسرته.
- مُشكلات نفسية وصحية نتيجة للتعرض للاحتيال والخداع، مع حالات من التوتر والقلق والاضطراب والاكتئاب، وما يُصاحب ذلك من أمراض صحية بدنية وذهنية أخرى.
- استهداف الفئات المستضعفة من السكان خاصة كبار السن وذوي الدخل المنخفض، الذين يتم استهدافهم بسبب نقاط ضعفهم المُتصورة لدى المُجرمين، مثل افتقارهم للمعرفة بالمخاطر المالية.

وأخيراً، هناك تداعيات بيئية للجريمة الاقتصادية، خاصة المتصلة بارتكاب جريمة بيئية لتحقيق مكاسب مالية ومادية أو تجنب دفع تكاليف مرتبطة بالامتثال للوائح والالتزامات البيئية؛ أخذاً بعين

الاعتبار أن هذه الجرائم تُعد واحدة من أكثر أنواع الجريمة ربحاً وأسرعها توسعاً؛ إذ تشير التقديرات إلى أن 25% من السوق العالمية لتداول الحيوانات والنباتات غير شرعي. وفي سياق متصل، تتكبد الشركات التي تقوم بجرائم بيئية تكاليف مالية باهظة جراء اكتشافها. مثال على ذلك، تحملت شركة "فولكس فاغن" الألمانية لصناعة السيارات خسائر وغرامات مالية قدرها 34.69 مليار دولار لاستخدامها برنامجاً إلكترونياً يقوم بتزييف البيانات الخاصة باختبارات انبعاثات غازات الدفيئة من سياراتها.

وعلى نطاق أشمل، تضم التداعيات البيئية للجريمة الاقتصادية أيضاً التأثير السلبي في الصحة العامة، واستنزاف الموارد الطبيعية الناضبة مثل: الغابات والمعادن. هذا إلى جانب فقدان التنوع البيولوجي في حال الإضرار بالموائل، وزيادة انبعاثات غازات الدفيئة التي تُغذي التغيُّر المُناخي.

ثالثاً: الاحتيال المالي المؤيد بالذكاء الاصطناعي – دراسة حالة

تُعد الجريمة الاقتصادية المدعومة سيبرانياً (Cyber-enabled Economic Crime) واحدة من أكثر الاتجاهات التي يشهدها عالم الجريمة الاقتصادية خطورة؛ لأنها تدمج بين ثلاث فئات منها، وهي الهجمات السيبرانية والاحتيال المالي وغسل الأموال. وفيما يخص ديناميكية العلاقة بينها، فعادة ما يتم ارتكاب جريمة سيبرانية لتسهيل عملية احتيال مالي، ترافقها لاحقاً عملية غسل للأموال التي تم اكتسابها احتيالياً لإضفاء الشرعية عليها. ولا عجب أن الذكاء الاصطناعي يؤدي دوراً رئيساً في ارتكاب هذه الجريمة المُركبة، حتى تنامى استخدام مصطلحات مثل "تصنيع الاحتيال" و"اقتصادات الاحتيال".

1. تصنيع الاحتيال واقتصاداته: تعود أول جريمة احتيال مالي مؤيدة بالذكاء الاصطناعي، تم الإبلاغ عنها لشهر مارس 2019؛ إذ استخدم المُحتالون تقنية "التزييف العميق" لإيهام الرئيس التنفيذي لشركة ما، تعمل في قطاع الطاقة بالمملكة المُتحدة أنه يتحدث هاتفياً للرئيس التنفيذي للشركة الأم في ألمانيا، الذي أمره بتحويل مبلغ 234 ألف دولار لمُورد ما، في دولة المجر في غضون ساعة واحدة لأمر عاجل. وبالفعل تم تنفيذ التحويل المصرفي للمُورد المزعوم، الذي أعاد تحويل المبلغ لمصرف آخر في دولة المكسيك؛ ليتم تحويله بعد ذلك لمواقع جغرافية أخرى، وحتى الآن، لم تتعرف سلطات التحقيق على مُرتكبي هذه الجريمة.

جاءت هذه الحادثة لتعكس التحدي الجديد الذي يُواجهه العالم، حتى أوضح تقرير "احتيال الهوية" (Identity Fraud Report) الصادر عن شركة "سومسوب" ارتفاع عدد عمليات احتيال الهوية بواسطة تقنية "التزييف العميق" خلال عام 2023 لتُسجل عشرة أمثال ما كانت عليه في العام السابق عليه. كما خلصت بيانات صادرة عن منظمة "سيفاس" (Cifas) -وهي منظمة خدمية غير ربحية لمنع الاحتيال في المملكة المُتحدة- إلى ارتفاع حالات استخدام الذكاء الاصطناعي للاحتيال على الأنظمة المصرفية بنسبة 84% خلال عام 2022 مقارنة بالعام السابق عليه.

تؤكد هذه المؤشرات وغيرها التطور العملياتي لجرائم الاحتيال المالي المؤيدة بالذكاء الاصطناعي، التي يُلقي الإطار رقم (1) الضوء على بعض منها؛ لأنها تتسم بدرجة أعلى من الكفاءة والتخصص مع الاستفادة من أدوات وأساليب مُتقدمة. لذلك، ظهر مصطلح "تصنيع الاحتيال" ليُعلن تحُّول هذه

الجريمة إلى صناعة مُتطورة، تتسم بعدد من الخصائص الرئيسة -يُلخص أهمها الإطار رقم (2) – مثل: اتساع نطاق الفئات المُستهدفة والتخصص وتقييم العمل. كذلك، أضحى "الاحتيال بمثابة خدمة" (Fraud-as-a-Service) يُمكن الحصول عليها ممن يمتلك مقوماتها ومهاراتها، تماماً مثل الخدمات المشروعة التي ينتجها الاقتصاد الرسمي كالخدمات الاستشارية.

إطار (1): نماذج لجرائم مالية مؤيدة بالذكاء الاصطناعي

- هجمات إلكترونية متطورة (Sophisticated Cyberattacks): استخدام الخوارزميات والتقنيات المؤيدة بالذكاء الاصطناعي لشن هجمات إلكترونية مُعقدة على المؤسسات المالية، مثل: البرامج الضارة (Malware)، وبرامج الفدية، والتصيد الاحتيالي؛ إذ يُمكن للذكاء الاصطناعي أتمتة تقنيات الهجوم، وتخطي التدابير الأمنية التقليدية، والتكيُّف مع الاستراتيجيات الدفاعية القائمة؛ ما يزيد من صعوبة مواجهتها.

- التلاعب الخوارزمي بعمليات التداول (Algorithmic Trading Manipulation): يُمكن استغلال خوارزميات الذكاء الاصطناعي للتلاعب بالأسواق المالية عن طريق استراتيجية "التداول سريع التردد" (High-Frequency Trading, HFT). مثال لذلك، أن تقوم روبوتات التداول المُؤيدة بالذكاء الاصطناعي بتنفيذ عمليات تداول بسرعة البرق، استناداً إلى خوارزميات مُحددة مُسبقاً لإنشاء تحركات مُصطنعة بالسوق؛ ما يؤدي إلى تشوه أسعار السوق وتضليل المستثمرين الشرعيين وتكبدهم خسائر مالية.

- تضليل عملية تعقب التداول الداخلي (Insider Trading Detection Evasion): تتيح خوارزميات الذكاء الاصطناعي للمتداولين الداخليين تجنب الكشف عن عمليات التداول الداخلي القائمة على تحليل كميات هائلة من البيانات لتحديد اتجاهات التداول وحالات الشذوذ القائمة؛ ما يزيد من صعوبة اكتشاف أنشطة التداول غير القانونية من قِبل المُنظمين وفرق الامتثال، ويُقوض سلامة السوق.

- الاحتيال في التصنيف الائتماني (Credit Scoring Fraud): عبر أنظمة تسجيل التصنيف الائتماني المستندة إلى الذكاء الاصطناعي، يُمكن للمُحتالين التلاعب بخوارزمياته لإنشاء هويات اصطناعية، وتزوير المعلومات الائتمانية للحصول على قروض أو بطاقات ائتمانية أو رهون عقارية بأسلوب احتيالي؛ الأمر الذي يفضي إلى قيام المؤسسات المالية بمنح تسهيلات ائتمانية لأفراد غير مؤهلين أو ذوي مخاطر مرتفعة؛ مما يزيد من معدلات التخلف عن السداد، ويتسبب في خسائر مالية وإضرار بسمعة المؤسسة والجهاز المصرفي ككل.

إطار (2): سمات رئيسة لتصنيع الاحتيال

- اتساع نطاق الفئات المستهدفة: تستهدف عمليات الاحتيال فئات متعددة من الضحايا، بما في ذلك الأفراد والمنظمات ومؤسسات الأعمال التي تنتمي لجميع الأنشطة الاقتصادية في آن واحد. وفي سبيل النفاذ إلى أكبر عدد ممكن من الضحايا، قد يتعاون المُحتالون عبر شبكات للجريمة المُنظمة لتنفيذ مخططات احتيالية في مواقع جغرافية أو أسواق متنوعة.

- التخصص وتقسيم العمل: فمن جهة، تشير التحليلات إلى أن هناك أدواراً مُحددة داخل النظام البيئي للاحتيال، مثل: توفير البيانات والمعلومات (عبر التصيد الاحتيالي وخرق البيانات كمثال)، واستخدامها في عمليات احتيال أكثر تعقيداً (عبر احتيال الهوية مثلاً)، ثم استغلال الأموال غير المشروعة وتحويلها إلى مناطق جغرافية أخرى، بالإضافة إلى أنشطة غسل هذه الأموال لإضفاء الشرعية المُصطنعة عليها. هذا إلى جانب مهمة التنسيق وتخطيط عمليات الاحتيال المُعقدة.

- ومن جهة أخرى، عادة ما يتخصص المُحتالون في ارتكاب أنواع مُحددة من هذه الجرائم. على سبيل المثال، تتخصص فئة بعينها في تنفيذ عمليات خرق البيانات، في حين تتخصص مجموعات أخرى في جرائم الاحتيال في الاتجار بالنباتات أو الحيوانات، بينما تركز مجموعات أخرى على عمليات الاحتيال المرتبطة بالأطعمة والمشروبات، وغيرها.

- توطين التقنيات المُتقدمة: يستند تصنيع الاحتيال إلى مُكون تكنولوجي عالي التقنية، بما في ذلك الذكاء الاصطناعي وتعلم الآلة وتحليل البيانات الكبيرة وغير ذلك من التطبيقات التي تُحول أنشطته من عمل "الهُواة" إلى "صناعة مُتقدمة. مثال على ذلك، عمليات الاحتيال المؤيدة بالهندسة الاجتماعية وتقنية التزييف العميق.

- تخطي حدود الدولة الوطنية: تتسم عمليات التصنيع الاحتيالي بكونها عابرة للحدود الوطنية؛ إذ يؤدي المُحتالون الذين يعملون ضمن النظام البيئي للاحتيال في بلدان وولايات قضائية عدة؛ لاستغلال الثغرات التنظيمية والتعقيدات القضائية والفجوات التنسيقية بين الأطراف الرسمية المختلفة.

- تقديم الاحتيال كخدمة: يُشير ذلك إلى إمكانية قيام المُحتالين المُحترفين ببيع أدواتهم وتقديم خدماتهم وخبراتهم إلى عملاء بحاجة إليها بمقابل مالي؛ مثل ما يحدث مع الخدمات المشروعة التي تقوم بتوفيرها الأنشطة الاقتصادية الرسمية.

ومع اتساع ساحة التصنيع الاحتيالي، تزايد الاهتمام بما يُطلق عليه "اقتصادات الاحتيال"، التي تأتي على غِرار "اقتصادات العمل" و"اقتصادات الطاقة" وغيرها، ويختص هذا الفرع من علم الجريمة الاقتصادية بتحليل النظام البيئي الهيكلي للأنشطة الاحتيالية، بما في ذلك المُحتالين والضحايا والأطراف الثالثة ذات الصلة من منظور اقتصادي؛ إذ يسعى إلى تحليل كل من:

- الأثر الاقتصادي والاجتماعي والبيئي لجرائم الاحتيال، وتدابير الكشف عنه ومكافحته.
- الدوافع والحوافز المالية التي تدفع الأفراد والمنظمات لارتكاب أعمال احتيالية، وتحليل الفوائد المحتملة منها مقابل المخاطر المتصلة بها، وتكاليف التخطيط والتنفيذ.
- الخسائر المالية المباشرة والتكاليف غير المباشرة التي يواجهها الضحايا؛ مثل الإضرار بالسمعة والرسوم القانونية وغيرها.

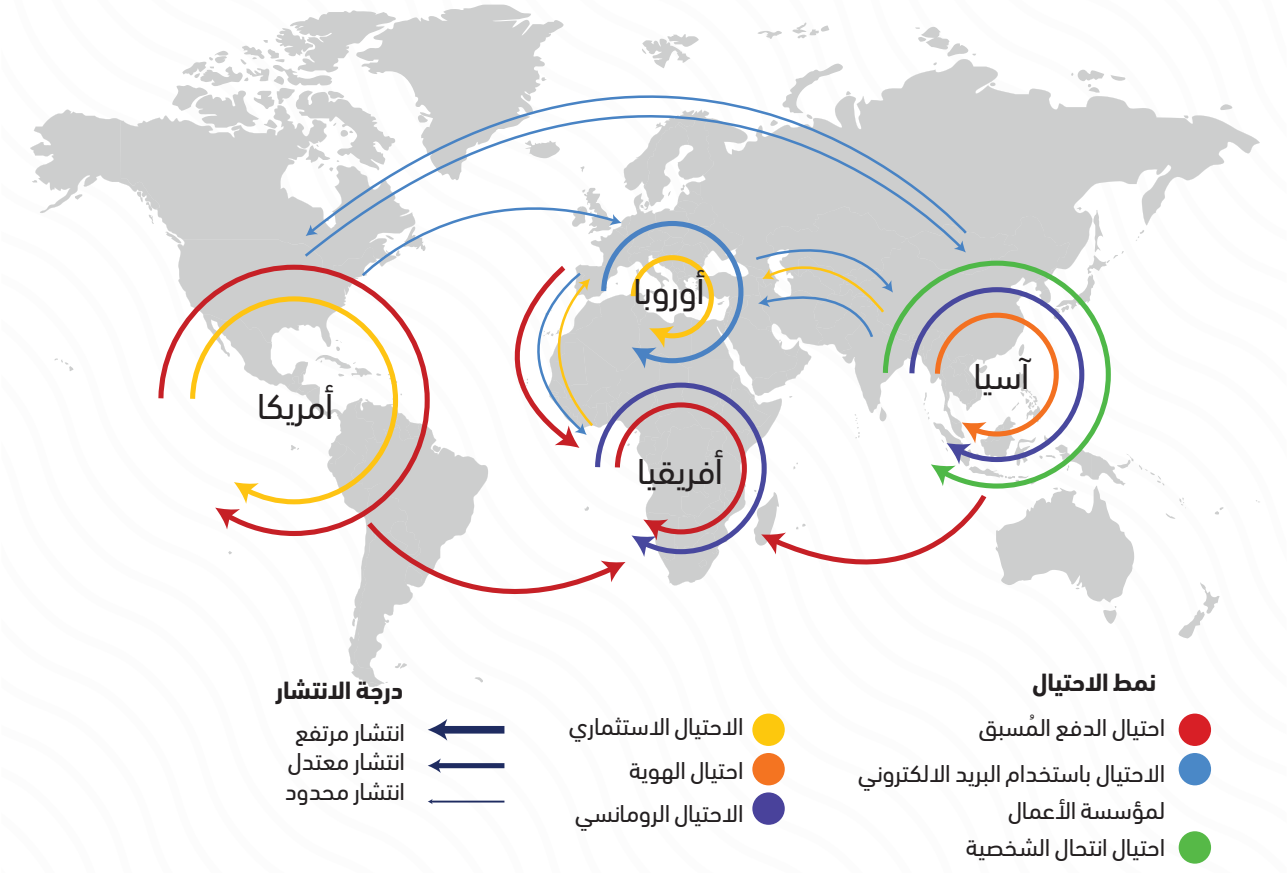
2. جغرافية الاحتيال المالي: أكد تقييم صادر في مارس 2024 عن "منظمة الشرطة الجنائية الدولية" (The International Criminal Police Organization – INTERPOL) بشأن الاحتيال المالي العالمي أن الاستخدام المتزايد للتقنيات المُتطورة –خاصة الذكاء الاصطناعي- قد مكَّن مجموعات الجريمة المُنظمة من استهداف الضحايا في جميع أنحاء العالم بشكل فعال، وجعل جرائم الاحتيال أكثر تعقيداً واحترافية دون الحاجة إلى مهارات تقنية متقدمة، وبتكلفة منخفضة نسبياً. وقد جاءت جرائم الاحتيال الاستثماري، والاحتيال في الدفع المسبق، والاحتيال الرومانسي، والاحتيال عبر استخدام البريد الإلكتروني لمؤسسات الأعمال في مُقدمة الجرائم الأكثر انتشاراً.

جغرافياً، وكما يُوضح الشكل رقم (4)، يُعد الاحتيال عن طريق إصدار أوامر دفع مُسبق زائفة واحداً من أكثر جرائم الاحتيال المالي انتشاراً في إفريقيا، كما ينتشر ارتكاب هذا النوع من الجرائم في بلدان الغرب والجنوب باستهداف ضحايا من خارج القارة. كما تشهد القارة الإفريقية أيضاً ارتفاعاً في جرائم الاحتيال الرومانسي (العاطفي) التي تستغل مستخدمي وسائل التواصل الاجتماعي وشبكة الإنترنت لإيقاعهم في علاقة عاطفية تنتهي بخداعهم والاحتيال عليهم.

وتُعد جرائم الاحتيال عبر أوامر الدفع المسبق والاحتيال الاستثماري الأكثر انتشاراً في الأمريكتين؛ إذ تنطوي الأخيرة على اتصال المجرمين دون ترتيب مُسبق بالضحايا لإقناعهم بالاستثمار في مخططات استثمارية أو شراء مُنتجات لا قيمة لها أو غير موجودة بالأساس. وفي البلدان الأوروبية –كما يُشير تقرير الإنتربول– تتفاقم جرائم الاحتيال الاستثماري والتصيُّد الاحتيالي، وسائر أنماط الاحتيال المالي عبر شبكة الإنترنت وتطبيقات الهاتف النقال؛ إذ يتم عادة انتقاء الضحايا بعناية لاستغلالهم إلى أقصى درجة.

وفي آسيا، يُعد "الاحتيال المالي عبر انتحال الشخصية" الأوسع انتشاراً؛ وفيه يتظاهر مرتكب الجريمة بأن لديه سلطة (على سبيل المثال مدير أو رئيس تنفيذي) تُخول له توجيه شخص ما في جهة العمل لدفع مبلغ مالي لطرف ثالث، وذلك عن طريق اتصال هاتفي أو بريد إلكتروني أو غير ذلك من أدوات التواصل الإلكتروني. هذا بالإضافة إلى انتشار كل من احتيال الهوية والاحتيال الرومانسي، وحوادث احتيال الدفع المسبق التي تستهدف بها البلدان الإفريقية، وحوادث الاحتيال عبر البريد الإلكتروني لمؤسسات الأعمال والاحتيال الاستثماري الذي تُستهدف به البلدان الأوروبية والأمريكية.

شكل (4): منظمة الشرطة الجنائية الدولية: الاتجاهات الإقليمية للاحتيال المالي



Source: INTERPOL. (2024, March 11). INTERPOL Financial Fraud assessment: A global threat boosted by technology. https://tinyurl.com/bdftttum

جديـر بالذكـر أن "تقريـر الجرائـم الماليـة العالميـة لعـام 2024" (Global Financial Crime 2024 Report) الصـادر عـن شركـة تكنولوجيـا الجرائـم الماليـة (Verafin) المملوكـة لشركـة "ناسـداك" الأمريكيـة يُظهـر أن عمليـات الاحتيـال ومخططـات الاحتيـال المصرفي (مثـل الاحتيـال عبر الشـيكات المصرفيـة وبطاقـات الدفـع والائتمـان المصرفي) بلـغ إجمـالي خسـائرها 485.6 مليـار دولار على مسـتوى العالـم خلال عـام 2023؛ منهـا 221.4 مليـار دولار خسـائر عمليـات الاحتيـال في منطقـة آسيا-الباسـيفيك لتُمثـل 45.6% مـن إجمـالي الخسـائر العالميـة. في حين سـجلت الأمريكتـان خسـائر بقيمـة 151.1 مليـار دولار (31.1% مـن الإجمـالي)، ومُنيـت بلـدان الشرق الأوسـط وشرق آسـيا بخسـائر قيمتهـا 113.1 مليـار دولار (22.3% مـن الإجمـالي).

رابعاً: دور الذكاء الاصطناعي في مكافحة الاحتيال المالي

في خضم الحرب ضد صناعة الاحتيال المُتطورة، التي تضر بالرفاه المالي للأفراد والمؤسسات والمجتمعات، وسلامة واستقرار النظام المالي بأكمله. أصبح تخصيص مزيد من الاستثمارات لإنتاج وتوطين تقنيات الذكاء الاصطناعي للكشف عن "الجريمة الاقتصادية المُمكنة سيبرانياً" واحداً من أهم الاتجاهات الكبرى لصناعتي الخدمات المالية والتكنولوجيا المالية بوصفه الأداة الأهم لتغيير قواعد اللعبة في خِضم الحرب ضد المُحتالين. وفي هذا السياق، يُعدُ الكشف عن الاحتيال المالي ومنعه في مقدمة أولويات العديد من الأطراف المتأثرة كالحكومات والشركات.

1. الكشف عن الاحتيال المالي ومنعه: يُمكن الوقوف على عدة أدوات وتقنيات مؤيدة بالذكاء الاصطناعي وتعلم الآلة، تساعد على الكشف عن الاحتيال المالي ومنعه، واللافت للاهتمام أنها تتكامل وتتقاطع فيما بينها، كما يتيح استخدامها وفق نهج شامل ومُنسق تحقيق مستوى أعلى من الفعالية في مُعالجة تحديات الجريمة المالية، بما في ذلك الخدمات المصرفية عبر الإنترنت وتطبيقات الهاتف المحمول ومعاملات البطاقات. ويأتي في مُقدمة هذه الأدوات والتقنيات ما يلي:

- **خوارزميات الكشف عن الاحتيال:** تُتيح تحليل بيانات المعاملات المالية وسلوكيات العُملاء لتحديد الأنماط الدالة على السلوك الاحتيالي وكشف الحالات الشاذة؛ بما في ذلك التعرف على الأنماط غير المُعتادة، أو تكرار معاملات غير نمطية، أو انحرافات في السلوكيات المُعتادة للعملاء؛ مثل مُحاولات تسجيل الدخول غير الناجحة المُتعددة على الحسابات المصرفية، والتغيُّرات المُفاجئة في أنشطة الحساب المصرفي.
- **نماذج تعلُّم الآلة:** تُستخدم للتعلم باستمرار من البيانات التاريخية لتحسين دقة وفعالية عمليات الكشف عن الأنشطة الاحتيالية بمرور الزمن، كما يُمكن استخدام المعرفة المُتولدة لديها في التكيُّف مع أنماط وسلوكيات الاحتيال المُستجدة والتنبؤ بها.
- **مصادقة المستخدم:** تعمل أنظمة المصادقة المستندة إلى الذكاء الاصطناعي على التحقق من هويات المستخدم ومنع الوصول غير المصرح به إلى الحسابات والأنظمة والبيانات المالية. وفي هذا السياق، يُمكن استخدام البيانات الحيوية التي تعتمد على السمات الجسدية مثل: التعرف على ملامح الوجه وبصمة الإصبع، و/أو القياسات الحيوية السلوكية التي تنطوي على تحليل وقياس أنماط السلوك الفردي التي يصعب على المُحتالين تقليدها أو تكرارها؛ مثل: نمط كتابة بيانات المستخدم أثناء عمليات تسجيل الدخول أو التعرف على الصوت.
- **مراقبة المُعاملات في الوقت الفعلي:** تُراقب أنظمة الكشف عن الاحتيال المؤيدة بالذكاء الاصطناعي تتبع المعاملات فور حدوثها في الوقت الفعلي، ما يُعد عنصراً حاسماً لمنع الأنشطة الاحتيالية في القطاع المصرفي والمالي وفق نهج استباقي.
- **التحليل السلوكي:** يُساعد على تتبع الانحرافات عن السلوك الطبيعي للعملاء وإظهار الأنشطة التي لا تتوافق مع الأنشطة النموذجية لهم عبر الزمن؛ بهدف تقييم سلوك العملاء والكشف عن الأنشطة المالية غير المُتسقة أو المشبوهة.

هـذا وتجـدر الإشـارة إلى أن غالبيـة هـذه الأدوات والتقنيـات تعتمـد في الأسـاس على تقنيـة "الدردشـة التحويلية التوليديـة المُدربـة مُسـبقاً" (Chat Generative Pre-trained Transformer, Chat GPT)، التـي تنتمـي لعائلـة "الـذكاء الاصطناعـي التوليـدي"، ويتـم تدريبهـا مُسـبقاً باسـتخدام كميات ضخمـة مـن البيانـات التاريخية لفهم الأنماط والسـلوكيات وإنشـاء اسـتجابات مُناسـبة. بالإضافة إلى ذلـك، فقد تنامى اعتمـاد هذه التقنيـات على "نماذج اللغـات الكبيرة المُدربـة الرأسـية" (Verticalized Trained Large Language Models, LLMs) التي تتسـم بأنها مُتخصصـة في مجال الكشـف عن الاحتيـال المالي حتى تكـون نتائجها أكثر فعاليـة، وذلك على نقيض "نمـاذج اللغات الكـبيرة الأفقيـة" -مثـل برنامـج الدردشـة (ChatGPT)- التي تتسـم بعمومية الموضوعـات التـي تتعامل معها.

2. تطبيقـات وأدوات لمكافحـة الاحتيـال المالي: في ظـل الاتجـاه المُتنامـي لإنتـاج وتـوطين تقنيـات مؤيـدة بالـذكاء الاصطناعـي للكشـف عـن الاحتيـال المالي والحـد منـه، يُمكـن الوقـوف على كـثير مـن الحـالات الفعليـة في هـذا السـياق. مثـال على ذلـك، أطلـق قسـم الجريمـة الماليـة وإدارة المخاطـر وكشـف الاحتيـال التابـع لشركـة "سـيمفوني للـذكاء الاصطناعـي" الأمريكيـة (SymphonyAI) برنامـج "سينسـا كوبايلـوت" (Sensa Copilot) لدعـم المُحقـقين في حـوادث الجرائـم الاقتصاديـة والماليـة مثـل: غسـل الأمـوال والاحتيـال المالي والاتجـار بالـبشر واسـتغلال الأطفـال والسرقـة والاتجـار بالحيـاة البريـة.

ويُعـد هـذا التطبيـق الأول مـن نوعـه الـذي يسـتخدم الـذكاء الاصطناعـي التوليـدي الـرأسي لدعـم جهـود الكشـف عـن الجرائـم الماليـة وإدارة تحقيقاتهـا مـن خلال جمـع المعلومـات الماليـة اللازمـة ومعلومـات مـن قِبـل الأطـراف الثالثـة، وعقـد مقارنـات فيمـا بينهـا وتلخيـص النتائـج التـي يتـم التوصـل إليهـا تلقائيـاً. ولزيـادة فعاليـة هـذا البرنامـج، قامـت الشركـة بعقـد شراكـة استراتيجيـة مـع شركـة "مايكروسـوفت" لدمـج خدمـة "أزور الـذكاء الاصطناعـي المفتـوح" (Azure OpenAI) بالبرنامـج.

في سـياق متصـل، اتجهـت شركات مثـل: "أدوبـي" و"مايكروسـوفت" و"جوجـل" بالفعـل لدمـج تقنيـة الـذكاء الاصطناعـي في المنتجـات التـي تُقدمهـا لقطـاع الأعمـال؛ لتُصبـح ذات اسـتخدامات مُتعـددة. كمـا تقـوم الشركات بـإطلاق مزيـد مـن الابتـكارات بـوتيرة متسـارعة، حتـى إن شركـة "البحـوث والأسـواق" (Research and Markets) تتوقـع بـأن سـوق الـذكاء الاصطناعـي العالميـة سـوف تنمـو خلال الـفترة مـن 2024 إلى 2030 بمعـدل نمـو سـنوي مُركـب 33.8%، لتصـل قيمتهـا إلى 1.057 تريليـون دولار بحلـول عـام 2030، مقارنـة بنحـو 137.7 مليـار دولار أمريكـي في 2023.

كذلـك، شرعـت الشركات الرائـدة في المدفوعـات الماليـة إلى تكثيـف اسـتثماراتها في تطويـر حلـول وتطبيقـات مؤيـدة بالـذكاء الاصطناعـي لدعـم جهـود الكشـف عـن الاحتيـال المالي والحـد منـه. ففـي أوائـل فبرايـر 2024، أعلنـت شركـة "مـاستركارد" للمدفوعـات الماليـة عـن تطويـر نموذجهـا المُؤيـد بالـذكاء الاصطناعـي التوليـدي لتعزيـز وسـائل الحمايـة التـي تُحافـظ على أمـان عملائهـا وشـبكة مدفوعاتهـا بالكامـل مـن أنشـطة الاحتيـال المالي؛ ويُتيـح النمـوذج الـذي أطلقـت عليـه مُسـمى (Decision Intelligence Pro) للبنـوك تقييـم المعـاملات الماليـة على شـبكتها بشـكل أفضـل في الوقـت الفـعلي.

تقـوم تقنيـة "مـاستركارد" الجديـدة بمسـح تريليـون نقطـة بيانـات؛ للتنبـؤ بمـا إذا كانـت المعـاملات المالية مشروعـة أم لا في أقـل مـن 50 ملي ثانيـة، مـع تدريـب خوارزميـات النمـوذج على مـا يقـرب مـن 125 مليـار معاملـة تتـم عبر شـبكة بطاقـات الشركـة سـنوياً لزيـادة درجـة دقتهـا؛ الأمـر الـذي يسـهم في تحـسين قـدرة

البنـوك على حمايـة حـاملي البطاقـات مـن المعـاملات الاحتياليـة، والتخفيـف مـن نتائـج "الإيجابيـات الكاذبـة" (False Positives) التـي تـدل على معـاملات مشروعـة يتـم تصنيفهـا بشـكل خاطـئ على أنهـا احتياليـة.

في مـارس 2024، أعلنـت شركـة "فيـزا" أيضـاً عـن تطويرهـا لثلاثـة تطبيقـات جديـدة مدعومـة بالـذكاء الاصطناعـي ضمـن مجموعـة الحمايـة الخاصـة بهـا (Visa Protect) للحـد مـن الاحتيـال في عمليـات الدفـع الفـوري بين الحسـابات والمعـاملات مـن دون بطاقـات الخصـم والائتمـان المصرفيـة، والمعـاملات داخـل وخـارج شـبكة مدفوعـات الشركـة، والمتمثلـة في الآتـي:

- توسـيع نطـاق المُصادقـة السـابقة عـلى المدفوعـات عـبر "فيـزا" عـبر أدوات مثـل: "تصديـق فيـزا المتقـدم" (Visa Advanced Authorization) و"مديـر مخاطـر فيـزا" (Visa Risk Manager)؛ ممـا يسـمح للجهـات الماليـة بتبسـيط عملياتهـا للكشـف عـن الاحتيـال.
- حمايـة تحويـلات حسـاب إلى حسـاب في الوقـت الفعـلي، والمُصممـة خصيصـاً للمدفوعـات الفوريـة؛ بمـا في ذلـك المحافـظ الرقميـة وأنظمـة الدفـع الفوريـة للبنـوك المركزيـة.
- المُصادقـة العميقـة مـن فيـزا (Visa Deep Authorization): وذلـك لمواجهـة الاحتيـال الرقمـي؛ إذ يُعـدُ هذا التطبيـق الجديـد أداة لتصنيـف مخاطـر المعامـلات الماليـة الرقميـة لإدارتهـا بشـكل أفضـل دون تعطيلهـا، اعتمـاداً عـلى نمـوذج الشـبكة العصبيـة مُتكـررة التعلـم العميـق (Recurrent Neural Network) بالإضافة إلى أداة "بتابايـت مـن البيانـات السـياقية" (Petabytes of Contextual Data).

وعلى مسـتوى القطاع المصرفي ككل، تكتسـب "المبادرات المصرفية المفتوحة" (Open Banking Initiatives) زخمـاً لدمجهـا بالأنظمـة المصرفيـة في بلـدان عالميـة مختلفـة؛ وهـي تسـمح بخفـض الحواجز أمام مشـاركة البيانـات الماليـة مـن خلال "واجهـات برمجـة التطبيقـات" (Application Programming Interfaces) المصرفيـة المفتوحـة الآمنـة والمُوحدة؛ ويعزز هذا الشـفافية والابتـكار في الخدمـات المالية، بالإضافـة إلى أنه يزيد مـن كفـاءة وفعاليـة أنشـطة الكشـف عـن الاحتيـال المالي والحـد منـه. مثـال على ذلك، تسـمح هـذه المبادرات بمشـاركة البيانـات الخاصة بسـجل المعـاملات المالية وأنمـاط الإنفاق من خلال هـذه الواجهات، التـي تزيد من القـدرة على إنتـاج تحلـيلات أكثـر عمقاً وأنمـاط أكثر دقة للكشـف عن الأنشـطة المشـبوهة.

بالإضافـة إلى ذلـك، توفـر هـذه المبـادرات فرصـاً لشركات الطـرف الثالـث للحصـول على موافقـة للوصول إلى بيانـات العـملاء مـن خلال هـذه الواجهـات؛ ممـا يمكّنهـا مـن تقديـم خدمـات مخصصـة مثـل: تحليـل الميزانيـات وإدارة المال والقـروض. يُذكـر أن العديـد مـن الـدول قـد اعتمـدت المبـادرات المصرفيـة المفتوحـة، ومـن بينهـا: المملكـة المتحـدة، والاتحـاد الأوروبـي، وأستراليـا، وسـنغافورة، والبرازيل، والمكسـيك.

خامساً: تحديات وفرص مستقبلية

رغـم تسـارع جهـود الكشـف عـن الجريمـة الاقتصاديـة والماليـة ومكافحتهـا، والاسـتخدام المُتنامـي لتقنيـات الـذكاء الاصطناعـي مـن قِبـل المؤسسـات الماليـة والمصرفيـة وجهـات التحقيـق؛ فإنـه يُمكـن الوقـوف عـلى تحديـات وقيـود عـدة مـن جهـة، وفـرص سـانحة مـن جهـة أخـرى؛ لإضفـاء مزيـد مـن الكفـاءة والفعاليـة عليهـا، والتـي تدعـم التفـوق عـلى التهديـدات الناشـئة مـن قِبـل جماعـات المُحتالـين.

1. تحديات وقيود رئيسة: رغم التطور التقني والمعرفي في مواجهة الجريمة الاقتصادية والمالية؛ فإن الكشف عنها لا يزال مهمة صعبة ومُعقدة، وتحفها كثير من التحديات، يأتي في مقدمتها ما يلي:

- **الطبيعة العابرة للحدود:** مع زيادة درجة ترابط وتشابك الاقتصاد العالمي، زاد معدل الجريمة العابرة لحدود الدولة الوطنية، كما يتعمد مرتكبوها في أحيان كثيرة تجزئتها بين بلدان عدة حتى يصعب تعقبهم؛ لأن التعاطي معها في هذه الحالة سينطوي على أطر قانونية مختلفة وولايات قضائية مُتعددة، وتنسيق فعَّال بين وكالات إنفاذ القانون والهيئات التنظيمية.

يرتبط التعامل مع التحقيقات عابرة الحدود بعدد من التحديات، منها الرغبة في "الامتياز القانوني"؛ فقد تسعى أكثر من ولاية قضائية لتأكيد سيادتها على سير التحقيقات. أيضاً، قد تضع التحقيقات في بعض القضايا؛ الخصوصية الدستورية لدولة ما على المحك. ثمة تحدٍّ آخر يتعلق بمشاركة ونقل البيانات إلى خارج الدولة؛ مما قد يُعرض السمعة الاقتصادية للدولة وللمؤسسات التي يتم التحقيق معها للخطر ويُهدر الثقة بها.

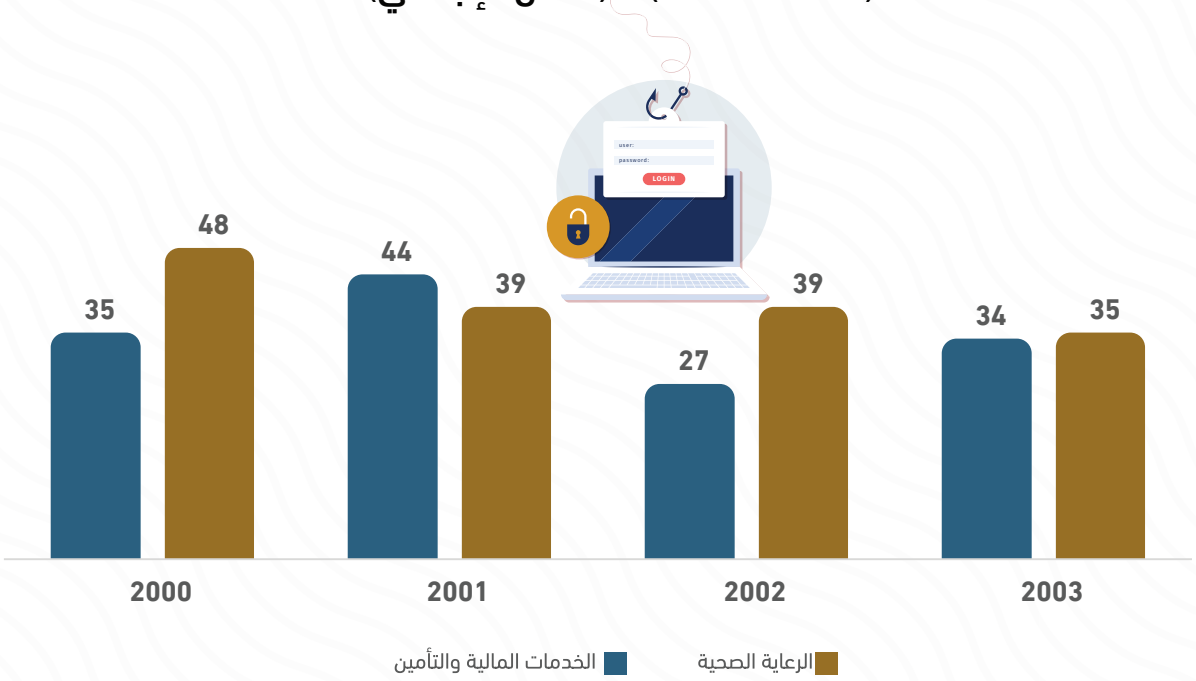
- **الامتثال التنظيمي:** تنطوي جهود مكافحة الجريمة الاقتصادية والمالية على وجوبية امتثال المؤسسات المختلفة لعدد كبير من اللوائح والمتطلبات التنظيمية المتعلقة بمكافحة الجرائم الاقتصادية، ومنها على سبيل المثال، مكافحة الفساد والرشوة وغسل الأموال وخصوصية وسرية البيانات والمعلومات وحماية المستهلك؛ الأمر الذي يُمثل عبئاً تنظيمياً على كثير منها، بالإضافة إلى افتقار بعضها –خاصة المؤسسات صغيرة ومتناهية الصغر– للموارد المالية والبشرية والتقنية اللازمة للكشف عن الجرائم الاقتصادية ومنعها بشكل فعَّال.

- **التهديدات الداخلية:** تُعد التهديدات الداخلية من قِبل أشخاص يعملون لصالح مؤسسة ما أو معها –مثل الموظفين والشركاء والموردين– إحدى أكبر التحديات الأمنية التي تواجهها المؤسسات؛ لما لدى أولئك الموظفين والشركاء والموردين من صلاحيات للنفاذ إلى البيانات والمعلومات والأنظمة التقنية، وما يقومون به من مهام ضمن دورة العمل؛ ولذلك، لا يقتصر تعقب الجريمة الاقتصادية ومنعها فقط على مكافحة المُتسللين من الخارج، ولكن أيضاً يجب تعقب المتسللين من الداخل.

جدير بالذكر أن تقرير شركة "فيرزون" الأمريكية للتحقيقات في خروق البيانات (The 2023 Verizon Data Breach Investigations Report, DBIR) لعام 2023 –الذي يغطي أكثر من 16300 حادثة؛ منها ما يزيد على 5 آلاف خرق للبيانات خلال الفترة منذ بداية نوفمبر 2021 وحتى نهاية أكتوبر 2022 – قد خلص إلى أن الفاعلين الداخليين قاموا بتسريب مليار عنصر بيان، مُقابل 200 مليون فقط وصل إليها فاعلون خارجيون؛ أي أنهم تسببوا في أضرار بلغت عشرين ضعف المُتسللين من خارج المؤسسة. كذلك فإن ما يزيد على 33% من خروقات البيانات في قطاع الخدمات المالية والتأمينية وقطاع الرعاية الصحية يُعزى لمُطلعين موثوقين من الداخل، كما يوضح الشكل رقم (5).

- **مواكبة مخاطر وتهديدات الجريمة الاقتصادية والمالية الناشئة:** ينبغي أن تسعى المؤسسات المالية والهيئات التنظيمية ووكالات الإنفاذ؛ لأن تكون في الصدارة دائماً في مقابل التطورات التي يُدخلها المُجرمون على الأدوات والتقنيات المُستخدمة في ارتكاب جرائمهم، وذلك لأنهم يستفيدون من التكنولوجيات المتقدمة، وتيارات العولمة التي توفر لهم فرصاً أكبر لمزاولة أنشطتهم غير المشروعة على نطاق دولي، بالإضافة إلى تزايد الاعتماد على المنصات الرقمية التي تزيد في المقابل من الهجمات السيبرانية.

شكل (5): تطور الأهمية النسبية لخروقات البيانات من قِبل فاعلين موثوق بهم من داخل المؤسسات في قطاعي الخدمات المالية والتأمين والرعاية الصحية (2020 – 2023) – (% من الإجمالي)



Source: Source: Denbigh-White, C. (2023, June 22). Seven Takeaways from the 2023 Verizon Data Breach Investigations Report. Next DLP :https://tinyurl.com/rz3zkatb

2. فرص مستقبلية: في مقابل التحديات والتهديدات التي تُخيم على عمليات مكافحة الجريمة الاقتصادية والمالية، توجد أيضاً فرص وإمكانات يُمكن التعويل عليها لكسب المعركة ضد صناعة الاحتيال، ويأتي في مقدمة هذه الفرص التعاون المُنسق والفعال بين الحكومة والقطاع المدني والمؤسسات المالية والمجموعات الصناعية لمكافحة هذه الجرائم على المستويين الوطني والدولي، ويتيح التعاون المشترك تبادل المعلومات المتعلقة بالتهديدات وأفضل الممارسات والرؤى بشأن اتجاهات الجريمة والخبرات المتميزة لاكتشافها ومنعها. كما أن الاعتماد على بيانات مجموعة من جهات عدة يُضفي على مدخلات ومُخرجات تقنيات الذكاء الاصطناعي مزيداً من الدقة والشمولية.

يُوفر التعاون المُشترك بين الجهات المختلفة أيضاً إمكانية إجراء عمليات التحقق المُتبادل من الأنشطة والمعاملات المشبوهة؛ ما يزيد من احتمالات التدخل في الوقت المُناسب لمنع الجريمة قبل حدوثها أو الحد من تداعياتها. أيضاً، يُساعد العمل المشترك بين المؤسسات على الاستفادة من وفورات الحجم؛ مما يخفض التكلفة الفردية التي يتحملها كل طرف، ويزيد من فعالية الإنفاق على الأدوات والتقنيات والعمليات الأكثر تطوراً لمكافحة الجريمة.

يُعد التعاون لتكثيف جهود المراقبة في الوقت الفعلي فرصة مهمة لتحديد الجرائم المالية ومنعها بشكل فعَّال. فمن خلال تحليل كميات ضخمة من بيانات المعاملات المالية والعملاء، يُمكن استنباط رؤى ذات قيمة بشأن الأنماط والاتجاهات ونقاط الشذوذ، كذلك فإن الاكتشاف المُبكر لها يساعد على إطلاق التنبيهات واتخاذ إجراءات للاستجابة الفورية مثل: حظر المعاملة أو توقيف الحساب المصرفي. بالإضافة إلى المزايا التي تتيحها عملية المراقبة في تتبع التغيرات في السلوكيات الاحتيالية للمجرمين للتعامل معها. جدير بالذكر أنه من المتوقع أن يتجاوز عدد مستخدمي الخدمات المصرفية الإلكترونية 3.6 مليار شخص خلال عام 2024؛ مما يزيد من أهمية مراقبة جميع معاملاتهم المالية آنياً.

وإلى جانب الفرص السانحة لتخصيص مزيد من الاستثمارات لإنتاج تقنيات وأدوات جديدة للكشف عن الجريمة الاقتصادية والوقاية منها، يظل من الضروري تهيئة البيئة التشريعية المساندة لاستخدام الذكاء الاصطناعي الآمن والإيجابي. من أمثلة هذه الجهود:

- **وثيقة "العملية هيروشيما للذكاء الاصطناعي" (Hiroshima AI Process):** أصدرتها مجموعة الدول السبع الصناعية في أكتوبر 2023 كمدونة سلوك طوعية للشركات التي تعمل على تطوير أنظمة الذكاء الاصطناعي المتقدمة؛ لتحقيق التوازن بين تعزيز الابتكار من جهة، وضمان السلامة والأمن من جهة أخرى، وتستهدف هذه المدونة أنظمة الذكاء الاصطناعي المتقدمة التي تستخدم نماذج أساسية مثل: الشبكات العصبية العميقة والذكاء الاصطناعي التوليدي الذي يُحاكي البشر أو يؤثر في سلوكياتهم.
- **إعلان "بليتشلي من أجل تطوير آمن للذكاء الاصطناعي" (Bletchley Declaration on AI Safety):** وقعته 28 حكومة في نوفمبر 2023، من بينها الصين والولايات المتحدة الأمريكية والاتحاد الأوروبي، وذلك تأكيداً للحاجة المُلحة لفهم وإدارة المخاطر المُحتملة للذكاء الاصطناعي وفق نهج جماعي يسعى إلى ضمان تطويره ونشره بطريقة آمنة ومسؤولة.

في سياق متصل، يُعدُ بناء القدرات وتنمية مهارات المؤسسات المالية والهيئات التنظيمية وجهات الامتثال فرصة رئيسة لصقل الخبرات المتخصصة في كشف الجريمة الاقتصادية والتحقيق فيها والوقاية منها؛ الأمر الذي ينطوي على مجالات عدة منها التدريب على تقنيات الكشف عن الاحتيال، والتحري والتحقيق، والطب الشرعي الرقمي، والأمن السيبراني، والمحاسبة الجنائية، وغير ذلك من أفرع "صناعة مكافحة الجريمة الاقتصادية"، والذي يتعين أن يتفوق على ممارسات "صناعة الاحتيال". كذلك، ينبغي أن تمتد جهود بناء القدرات إلى رفع مستوى الوعي بين أصحاب المصلحة والمواطن العادي وواضعي السياسات العامة، بشأن طبيعة الجريمة الاقتصادية وأنواعها ومخاطرها وتأثيراتها.

سادساً: ملاحظات ختامية

يُنذر نيك شارب، نائب مدير المركز الوطني للجريمة الاقتصادية (National Economic Crime Centre, NECC) بالمملكة المتحدة، بأن العالم لم يشهد حتى الآن استخدام الذكاء الاصطناعي في عمليات الاحتيال على نطاق واسع، الذي يُعد الخطر الأكبر الذي سيُواجه جهود مكافحة مثل هذه الجرائم؛ واللافت

للانتباه أن هذا التحذير يأتي في بدايات عام 2024 بعد أن عانى العالم بالفعل من تنامٍ غير مسبوق في معدلات الجريمة الاقتصادية بجميع فئاتها وحدوث تحولات عميقة في مشهد الجريمة الاقتصادية؛ ما يطرح تساؤلاً جوهرياً عما سيكون عليه الحال في المستقبل القريب.

لا يُمكن لشخص ما التنبؤ بدقة بما يحمله مستقبل الذكاء الاصطناعي لساحة الجريمة الاقتصادية، بيد أن هناك حقيقتان مؤكدتان. تتمثَّل الأولى في أن تطور الذكاء الاصطناعي يحدث وفق معدل أسرع بكثير مما توقعه الخبراء. لقد خلصت ورقة بحثية قامت بمسح ما يقرب من ثلاثة آلاف ورقة بحثية في مجال الذكاء الاصطناعي إلى أن متوسط التاريخ التقديري الذي سيتمكن فيه الذكاء الاصطناعي من التغلب على البشر في كل مهمة مُمكنة قد تغير بشكل كبير؛ ليصبح عام 2047 بدلاً من عام 2060؛ أي أنه تم اختصار هذا الفاصل الزمني بنحو 13 عاماً. في حين تُشير الحقيقة الثانية إلى أنه سيظل هناك دائماً سباق محموم للتسلح بتقنيات الذكاء الاصطناعي بين طرفي الجريمة الاقتصادية؛ المجرمين من جهة والقائمين على مكافحتها من جهة أخرى.

وفي ضوء ذلك، يُعلي تقرير "الإنتربول" أهمية العمل الحثيث للتخلص من أية ملاذات آمنة يلجأ إليها المحتالون، وسد الفجوات القائمة والتأكد من أن تبادل المعلومات بين القطاعات وعبر الحدود هو القاعدة وليس الاستثناء، وتشجيع المزيد من الإبلاغ عن الجرائم الاقتصادية والمالية؛ ليكتمل ذلك باقتناص كثير من الفرص السانحة لتعزيز جهود الكشف الفعال عنها والوقاية منها ومحاسبة مرتكبيها، والتي يأتي في مقدمتها تعزيز ثقافة التعاون والابتكار والاستخدام المسؤول للذكاء الاصطناعي، وبناء نظام أكثر تماسكاً ومرونة وتطوراً لمكافحة الجريمة.

المراجع بالترتيب الأبجدي:

المراجع باللغة العربية:

1. عوض، ر. م. (2023). الغسل الأخضر: المنطق وآليات المواجهة، مركز المعلومات ودعم اتخاذ القرار التابع لمجلس الوزراء المصري، مجلة آفاق المناخ، السنة الأولى، العدد الثالث، مايو.

المراجع باللغة الإنجليزية:

1. AFP. (2024, March 27). Visa's growing services business infused with new AI-powered products. **AFP**. https://tinyurl.com/ycypyznz

2. AIG. (2024). **Impersonation fraud claims scenarios**. https://tinyurl.com/3yash842

3. Al Helou, E. (2023, August 21). Embracing Open Banking: A gateway to fintech innovation in the Middle East. **Middle East Economy**. https://tinyurl.com/4a2j978z

4. AML Intelligence. (2024, January 16). More than $3 trillion in illicit funds flowed through global financial system in 2023; banks call for more regulatory guidance to tackle endemic. **AML Intelligence** https://tinyurl.com/yc3yr6ny

5. Beatman, A. (2023, December 14). Azure OpenAI Service powers the Microsoft Copilot ecosystem. **Microsoft Azure**. https://tinyurl.com/38s26hz9

6. Chapman, T. (2024, January 23). How AI is Changing the Financial Crime Landscape. **FinTech Magazine**. https://tinyurl.com/27vp3pms

7. Chen, H., & Magramo, K. (2024, February 4). Finance worker pays out $25 million after video call with deepfake 'chief financial officer'. **CNN**. https://tinyurl.com/yp5jf635

8. Cifas. (2023, April 12). **Identity fraud cases reach all-time high as cost-of-living crisis bites.** https://www.cifas.org.uk/newsroom/fraudscape23-release

9. Claver, C., El Khoury, C., & Weeks-Brown, R. (2023, December 7). **Financial Crimes Hurt Economies and Must be Better Understood and Curbed**. IMF. https://tinyurl.com/4hhm2wpk

10. Davison, T. (2024, February 8). Greenwashing Examples: The Nine Biggest Fines Handed Out So Far. **CleanHub**. https://blog.cleanhub.com/greenwashing-examples

11. Denbigh-White, C. (2023, June 22). **Seven Takeaways from the 2023 Verizon Data Breach Investigations Report**. Next DLP. https://tinyurl.com/rz3zkatb

12. Dinitz, S. (1976). Economic Crime. National Library of Medicine, **Quard Criminol Clin**, 18(4), 433-458. Italian.

13. Dinitz, S. (1977). Economic Crime. **US Department of Justice – Office of Justice Programs**.

https://tinyurl.com/yc6t6u3m

14. EMA. (2016, October). **The Industrialization of Fraud Demands a Dynamic Intelligence-driven Response**. https://www.images.shi.com/pdf/ema-rsa_industrializing-fraud-1016-wp.pdf

15. Encyclopedia.com. (2018, August 18). A Definition of White-Collar Crime. Retrieved from https://tinyurl.com/2svyunvb

16. EY. (2024). **Disrupting financial crime**. https://www.ey.com/en_gl/disrupting-financial-crime.

17. Financial Crime Academy. (2023, December 15). **Financial Crimes in Environmental Crimes.** https://tinyurl.com/3jf7k48e

18. Financier Worldwide Magazine. (2021, December). Navigating issues in cross-border investigations. Special Report on White-Collar Crime. **Financier Worldwide Magazine.** https://tinyurl.com/4djhzvmt

19. Finksus. (2023). **What are the Financial Crime Trends in 2023?** https://tinyurl.com/4f85rnmz

20. Hall, I. (2024, January 30). AI-enabled criminality 'probably' biggest growing risk in financial fraud battle. **Global Government FinTech**. https://tinyurl.com/2bptzzyz

21. Hart, N. T. (2022, November 3). **Street Crime vs. White-Collar Crime**. Harrison & Hart LLC. https://tinyurl.com/3smm6jt8

22. Hernandez, J.R. (2024). **What is the Actual Cost of Cybercrime. Evolve.** https://tinyurl.com/3te69mm8

23. Identity Theft Resource Center. (2019, September 16). **First-Ever AI Fraud Case Steals Money by Impersonating CEO**.

24. Imperva. (2024). **What is social engineering** https://tinyurl.com/3a9jxhwy

https://www.imperva.com/learn/application-security/social-engineering-attack/

25. INTERPOL. (2024, March 11). **INTERPOL Financial Fraud assessment: A global threat boosted by technology.**

https://tinyurl.com/bdftttum

26. Irwin, L. (2023, April 25). **Insider Threats Unveiled: Definition, Types, and Real-Life Examples**. IT Governance. Retrieved from https://tinyurl.com/4ydyra7k

27. KPMG. (2023, August). **Five ways AI can help manage economic crime risk more effectively**. https://tinyurl.com/yed9tmp5

28. Libatique, R. (2024, January 26). Report unveils emerging AI challenges in financial crime. **Insurance Business**. https://tinyurl.com/wpa8va2z

29. Mahmud, A. (2024). **5 AML regulations set to shape financial crime in 2024**. Comply Advantage. https://tinyurl.com/48ax6hvr

30. Management Solutions. (2024). **Financial Crime: Trends and Challenges in the Digital Era.** https://tinyurl.com/2bjsm6js

31. Mastercard Newsroom. (2024, February 1). **Mastercard supercharges consumer protection with gen AI.** https://tinyurl.com/5hd22u2r

32. Mojsoska, S., Nikolovska-Vrateovska, D., & Vrteovski, S. (2021, November 26). **The Economic Crime, Social Costs and Economic Growth.** https://eskup.kpu.edu.rs/dar/article/download/282/200

33. Mollick, E. (2024, January 6). **Signs and Portents: Some hints about what the next of AI looks like**. One Useful Thing. https://www.oneusefulthing.org/p/signs-and-portents

34. Odeyemi, O., et al. (2024, February 10). Reviewing the role of AI in fraud detection and prevention in financial services. **International Journal of Science and Research Archive**, 11(01), 2101–2110. Retrieved from https://tinyurl.com/2s3hxxuc

35. PwC. (2023). **PwC's Global Economic Crime and Fraud Survey** 2022. https://tinyurl.com/bdukdmut

36. PYMNTS. (2022, March 3). **Synthetic Identity Fraud Costs Businesses Billions Each Year**, Data Shows. https://tinyurl.com/5zdbxx5t

37. PYMNTS. (2024, April 8). **Oracle Introduces AI-Powered Anti-Money Laundering Service for Banks**. https://tinyurl.com/4u2nx5nk

38.Research and Markets. (2024, February). **Artificial Intelligence Market, Size, Global Forecast 2024-2030, Industry Trends, Share, Growth, Insight, Impact of Inflation, Company Analysis**. https://tinyurl.com/3t8ek93y

39. Sanction Scanner. (2024). **Environmental Crime and Money Laundering**. https://tinyurl.com/fd5jhyvu

40. SEON. (2024). **Fraud as a Service**. https://seon.io/resources/dictionary/fraud-as-a-service/

41. Simmons, C. (2024, February 5). **Top Trends in Anti-Financial Crime in 2024**. https://tinyurl.com/24mty3rp

42. Sjouwerman, S. (2024, January 23). Deepfake Phishing: The Dangerous New Face of Cybercrime. **Forbes**. Retrieved from https://tinyurl.com/5n6duybs

43. Stupp, C. (2019, August 30). Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case. **WSL Pro Cybersecurity**. https://tinyurl.com/3yhdsv2d

44. Sumsub. (2023, November 28). **Sumsub Research: Global Deepfake Incidents Surge Tenfold from 2022 to 2023**. https://tinyurl.com/489k9huz

45. The Government of Japan. (2024, February 9). **The Hiroshima AI Process: Leading the Global Challenge to Shape Inclusive Governance for Generative AI**. https://tinyurl.com/mv6wvvue

46. Thompsett, L. (2024, January 22). Sumsub: Identity Fraud up 73%; how can Fintechs React? **FinTech Magazine**. https://tinyurl.com/4uh2wkbe

47. Transform Finance. (2024, January 30). 7 FinCrime and Compliance Trends for 2024. **Transform Finance**. https://transformfinance.media/finance/trends-in-financial-crime-compliance/

48. UK Department for Science, Innovation and Technology. (2023, November 1). **The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023**. https://tinyurl.com/5n8kcxr3

49. UNIT21. (2024). **Financial Crime: Main Types, Consequences and Real-Life Examples**.

https://www.unit21.ai/fraud-aml-dictionary/financial-crime#section3

50. US Federal Trade Commission. (2022, December). **Equifax Data Breach Settlement.**

https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement

51. Venkataramakrishnan, S. (2024, January 19). AI heralds the next generation of financial scams. **Financial Times**. https://www.ft.com/content/beea7f8a-2fa9-4b63-a542-88be231b0266

52. Wade, M., Tomlinson, N., & Srinivas, V. (2024). **2024 Banking and Capital Markets Outlook**. Deloitte Insights. https://tinyurl.com/y35vk5rj

53. Wolf, B. (2024, February 20). AI, other technology the “only answer” to AML challenges in evolving threat landscape, says ACAMS report. **Thomson Reuters**. https://tinyurl.com/5dh538ak

54. Zandt, F. (2024, March 13). **How Dangerous are Deepfakes and Other AI-Powered Fraud?**. Statista. Retrieved from https://www.statista.com/chart/31901/countries-per-region-with-biggest-increases-in-deepfake-specific-fraud-cases/

عن المستقبل:

"المستقبل للأبحاث والدراسات المتقدمة"، هو مركز تفكير Think Tank مستقل، تأسس في 2014/4/4، في أبوظبي، بدولة الإمارات العربية المتحدة، للمساهمة في تعميق الحوار العام، ومساندة صنع القرار، ودعم البحث العلمي، فيما يتعلق باتجاهات المستقبل، التي أصبحت تمثل مشكلة حقيقية بالمنطقة، في ظل حالة عدم الاستقرار وعدم القدرة على التنبؤ خلال المرحلة الحالية، بهدف المساهمة في تجنب "صدمات المستقبل" قدر الإمكان.

ويهتم المركز بالاتجاهات التي يمكن أن تساهم في تشكيل المستقبل، على المدى القصير، خاصة الأفكار غير التقليدية والظواهر "تحت التشكيل"، مع التطبيق على منطقة الخليج، من خلال رصد وتحليل الاحتمالات الممكنة، للتفاعلات القائمة والتيارات القادمة، وتقدير البدائل المتصورة للتعامل معها، باستخدام مناهج التفكير المتقدمة، عبر أنشطة علمية تجمع بين الأكاديميين والممارسين، والشخصيات العامة، من داخل الإمارات وخارجها.

أنشطة المركز:

مجلة اتجاهات الأحداث: دورية أكاديمية فصلية، تهتم بتحليل اتجاهات المستقبل على المدى القصير، بما يتضمنه من تيارات وتطورات، متعددة الأبعاد، وذات تأثيرات استراتيجية، وذلك في مجالات اهتمام برامج المركز.

تقديرات المستقبل: تقديرات تصدر يومياً لتغطية أبرز التطورات الإقليمية والدولية المؤثرة على منطقة الشرق الأوسط.

بوابة المستقبل: موقع إلكتروني أكاديمي، يقوم بنشر تحليلات يومية، باللغتين العربية والإنجليزية، حول أهم الأحداث والتطورات الجارية في المنطقة والعالم، ويغطي الموقع إنتاج المركز المطبوع وأنشطته المختلفة، من لقاءات عامة وحلقات نقاشية، ويقدم خدمات علمية تتعلق بعروض الكتب والدراسات، وقواعد البيانات والخرائط السياسية.

تقرير المستقبل: نشرة يومية تتضمن أبرز التقديرات والتحليلات التي ينتجها باحثو المركز، أو ما ينشر على موقعه الإلكتروني أو الدورية التي تصدر عن المركز، وغيرها من الأنشطة والإصدارات، وترسل عبر البريد الإلكتروني.

دراسات المستقبل: سلسلة دراسات أكاديمية تصدر كل شهرين، وتركز كل دراسة على قضية واحدة تمثل ظاهرة صاعدة على المستوى الاستراتيجي تتسم بالتعقيد وتعدد الأبعاد، وتهيمن على الجدل العام في الشرق الأوسط والعالم.

دراسات خاصة: سلسلة دراسات غير دورية تركز على الظواهر الصاعدة، والمؤشرات المركبة والأفكار غير التقليدية، والاتجاهات القادمة التي ترتبط بالعالم قيد التشكل.

التقرير الاستراتيجي: تقرير يصدر سنوياً عن المركز، ويركز على الاتجاهات الرئيسية طويلة المدى التي تشكلت في الشرق الأوسط من خلال تفاعلات العام السابق، والتي يتوقع أيضاً أن تكون الأكثر تأثيراً في حالة الإقليم خلال العام التالي.

مؤشرات المستقبل: تقرير غير دوري يرصد ويُحلل أبرز المؤشرات وقواعد البيانات واستطلاعات الرأي العالمية والإقليمية.

رؤى عالمية: تهدف إلى عرض أبرز ما يُنشر في مراكز الفكر والمجلات والدوريات البحثية الغربية، من أفكار غير تقليدية واتجاهات صاعدة في مختلف المجالات السياسية والأمنية والاقتصادية وغيرها.

ملفات المستقبل: سلسلة ملفات تجميعية تصدر بشكل غير دوري، وتتناول أهم الأحداث والتحولات الإقليمية والدولية، التي تشغل اهتمام الجمهور وتتصدر نقاشات المجال العام وقت صدورها.

فعاليات المستقبل: ينظم المركز عدة فعاليات مثل (اللقاءات العامة، وحلقات النقاش، والدورات التدريبية).

ISSN: 2616-583X

المستقبل للأبحاث والدراسات المتقدمة
FUTURE for Advanced Research & Studies

www.futureuae.com