مجلة
البحوث والدراسات القضائية والقانونية

الجرائم المالية الإلكترونية
ودور أنظمة الذكاء الاصطناعي
في تعزيز أدلة الإثبات (*)

الدكتور/ إبراهيم محمد الزنداني

أستاذ القانون الجنائي المساعد المتخصص بالأمن
السيبراني والذكاء الاصطناعي والجرائم الإلكترونية

(*) ورقة عمل قدمت في الورشة المنعقدة بين وزارة العدل وحقوق الإنسان، والقطاع المصرفي- صنعاء- الخميس ٢٠ فبراير ٢٠٢٥م.

الملخص:

تهدف هذه الورقة العلمية إلى التعريف بالجرائم المالية الإلكترونية وبيان أنواعها وصورها وتسليط الضوء على التحديات التي تواجه القطاع المالي والمصرفي في العالم السيبراني وأبرز الجرائم المالية الإلكترونية التي تطال الكيانات والمؤسسات المالية، ثم تتحدث عن الذكاء الاصطناعي والركائز والنُهُج التي تدخل في مكونات أنظمة الذكاء الاصطناعي، كما تتطرق إلى ما يمكن أن تفعله تقنيات وأنظمة الذكاء الاصطناعي عند إساءة استغلالها في عالم المال والأعمال والنتائج الكارثية التي قد تتسبب بها، وكذا دورها الإيجابي في رفع كفاءة وجودة التحقيقات الجنائية، وطريقة عمل خوارزميات أنظمة الذكاء الاصطناعي، وتقنيات التعلم الآلي لدعم وتعزيز مصداقية الأدلة الرقمية، وتختم هذه الورقة ببعض التوصيات والمقترحات العامة لتعزيز التكامل بين التكنولوجيا والقانون، لضمان مواجهة فعالة للجرائم السيبرانية بشكل عام والجرائم المالية في عالم رقمي، التخلف عنه وعدم خوض غماره بدراية وبصيرة وتخطيط ودراسة لتجارب الدول السباقة في هذا المضمار، يعني حجز مقعد دائم في ذيل أمم وشعوب العالم.

المقدمـــة

مع مطلع الألفية الثالثة حدثت ثورة هائلة في عالم الخوارزميات تحررت فيها التقنيات التكنولوجية من التكاليف المادية المرتفعة التي كانت تعيق التقدم التكنولوجي في جميع المجالات، وفي عالم المال والأعمال كان التقدم والتطور التكنولوجي والمعلوماتي المتسارع هو القوة الدافعة للابتكار في الصناعة المالية التي نتج عنها سلسلة من التحولات في الخدمات المالية ووصولاً إلى الاقتصاد الرقمي الذي يشكل ركيزة أساسية في اقتصادات دول العالم، وعلى الرغم من الفرص والعوائد الثمينة التي حققها قطاع التكنولوجيا المالية والتي تمثلت في تطور وسائل الدفع الإلكتروني والاعتماد المتزايد على الأنظمة الرقمية في التعاملات المالية بعد تطور شركات الاتصالات ومقدمي خدمات الإنترنت وتطور التجارة الإلكترونية بالإضافة إلى انضمام مؤسسات القطاعين العام والخاص إلى سوق الخدمات المالية الرقمية، فإنها أيضاً جلبت معها مخاطر وتحديات خطيرة لعل أهمها على الإطلاق الجرائم المالية الإلكترونية التي تعتبر وبحق السلاح الصامت الذي قد يدمر اقتصاديات الدول والحكومات دون إطلاق رصاصة واحدة، كونها تستهدف المؤسسات المالية والمصرفية والشركات والأفراد على حد سواء، وهو ما يعرض الأمن الاقتصادي والاجتماعي للخطر، معتمدة بذلك على تقنيات متطورة ومعقدة وذكية لاختراق الأنظمة المالية وسرقة الأموال وتنفيذ عمليات التصيد الاحتيالي والتلاعب بالبيانات وغسيل الأموال وتمويل الأنشطة غير المشروعة عبر الإنترنت.

بينما وعلى الضفة المقابلة يغرق معشر إنفاذ القانون في جدليات ونظريات فقهية وقانونية وتجاذبات ونقاشات جانبية حول المراكز القانونية والاختصاصات متناسين أنهم يتعاملون مع رواد أعمال لغتهم الخوارزميات واللوغاريتمات وعالم افتراضي يسير بوتيرة عالية وسرعة فائقة فالثانية وأجزائها مهمة ولها ثمنها، وجل ما فهمناه منهم وما وصلنا من السوابق القضائية للدول الأخرى وما يثبته الواقع الذي فرضه التحول الرقمي في بلادنا أن عملهم محفوف بالمخاطر فالتأخر ثانية أو الغفوة لبرهة قد تكلفنا الكثير ونحن مطالبون دائماً كسلطة لإنفاذ القانون اللحاق بهذا الركب الذي يسبقنا بآلاف الخطوات.

المطلب الأول
الجرائم المالية الإلكترونية

أدى التطور المستمر للتكنولوجيا وتقنية المعلومات وسرعة تضخم قواعد البيانات ثم تقادمها مع الأنظمة الإلكترونية المستخدمة سريعاً إلى ازدهار الصناعة المالية وظهور العديد من النماذج المالية الناشئة على شبكة الإنترنت، وهو ما لم يكن في حسبان صناع القرار الذين كانوا منغمسين برسم السياسات الجنائية لذلك الواقع المستجد بدون إلمام متعمق بإمكانيات تلك التقنيات والتحولات التي ستكون عليها في المستقبل، ومن ثم فقد تعددت الآراء وتباينت في الأوساط الأكاديمية والمراكز البحثية حول مفهوم موحد لماهية الجرائم المالية الإلكترونية وما نميل إليه ونرجحه أن مصطلح الجرائم المالية الإلكترونية بمفهومها العام يعني «ارتكاب أفعال غير مشروعة تستهدف القطاع المالي بواسطة شبكات الاتصالات السلكية واللاسلكية والحواسيب والهواتف الذكية وغيرها من المعدات التقنية الطرفية الأخرى»، ووفقاً لذلك فإن الجرائم المالية الإلكترونية تنقسم إلى:

أ. **الجرائم المالية الحاسوبية والشبكية:** وتشير عادة إلى استهداف النظام المعلوماتي المالي عن طريق استخدام الأصول التقنية المملوكة للكيان المالي وتدمير النظام المعلوماتي المالي أو ارتكاب جرائم اختلاس أو الاحتيال أو التعدي الوظيفي أو السرقة (Zhang Jiufeng, Xiao Sa, Zhang Jifeng 2014)، أو التلاعب بالبيانات المخزنة على الحواسيب أو تمكين طرف ثالث للولوج إلى النظام المعلوماتي المالي عبر ثغرة أمنية يتم إفشاؤها أو إنشاؤها وصولاً إلى تحقيق النتيجة الجرمية، أي أن هذا النوع من الجرائم يتم عادة باستخدام أجهزة الحاسوب دون الحاجة إلى الاتصال بشبكة الإنترنت، وتتضمن مهاجمة أنظمة البنوك أو الشركات عبر الشبكة الداخلية واعتراض البيانات المالية أثناء انتقالها عبر الشبكات أو التجسس على التحويلات المالية بين الأنظمة المتصلة.

ب. **الجرائم المالية عبر شبكة الإنترنت:** وتشمل جميع أنواع الأعمال الإجرامية التي تنتهك الأنظمة المالية ومصالح الآخرين في الأنشطة التجارية المالية عبر الإنترنت، وهو ما يعني إلحاق الضرر بالنظام المالي الوطني وسلامة ممتلكات المواطنين وبأمن وسلامة شبكة الإنترنت في البلاد (Zhonglun Research Institute, 2018, p.

6)، وفي هذا النوع من الجرائم يتم الاعتماد على شبكة الإنترنت العام كأداة لتنفيذ تلك الجرائم التي تستهدف الخدمات المصرفية عبر الإنترنت كاختراق التطبيقات الإلكترونية مثل المحافظ الإلكترونية وماكينات ATM وبث البرمجيات الخبيثة DoS في الأنظمة المعلوماتية المالية بهدف تعطيل توافر تلك الخدمات وقرصنة الأنظمة المعلوماتية البنكية المتعلقة بالحسابات المصرفية، وتدميرها بحيث تكون غير قابلة للاستخدام، وانتحال الشخصية واستخدام البطاقات البنكية المزورة، وكذا استغلال العميل لثغرة أمنية تمكنه من الاستيلاء على أموال لا علاقة له بها أو سرقة وقرصنة المصنفات الرقمية والملكيات الفكرية ذات القيمة المادية الكبيرة، أضف إلى ذلك استخدام أنظمة وتقنيات الذكاء الاصطناعي للتأثير على التجارة الإلكترونية، والاستثمار في الأسواق العالمية عبر الإنترنت عن طريق التلاعب بأسواق الأسهم والأوراق المالية والبورصات، وكذا استهداف منصات الدفع الإلكترونية الوطنية والأجنبية بعمليات احتيالية وسرقة بيانات المودعين واختراق الأنظمة المالية بهدف الولوج إليها عبر الثغرات الأمنية والاستيلاء على الأموال وتنفيذ هجمات الفدية، واستخدام شبكة الإنترنت لارتكاب جرائم غسيل الأموال ودعم الأنشطة غير المشروعة ...إلخ.

المطلب الثاني
صور الهجمات السيبرانية الواقعة على القطاعات المالية والمصرفية

الحقيقة أن الهجمات السيبرانية على القطاع المالي والمصرفي باتت من القضايا التي تؤرق الدول في العالم السيبراني، ولمعرفة التطور المستمر في الجرائم المالية الإلكترونية عبر شبكة الإنترنت تشير إحصائيات جرائم الاحتيال المالي في العام ٢٠٠٦م ونسبتها من عدد الجرائم السيبرانية في بعض الدول الفاعلة في الاقتصاد العالمي على النحو التالي: الولايات المتحدة الأمريكية حوالي ٣٠٪ ، الصين ٢١,٦٪، كوريا الجنوبية ١١,٥٪، البرازيل ٥,١٪، الاتحاد الروسي ٣,٥٪، ألمانيا ٢,٥٪، إسبانيا ٢,٢٪، كندا ١,٥، اليابان ١,٤٪، بريطانيا ١,٤٪ (InterCrime-Press: all about money, **25.04.2006**, https://www.icpress.ru)، وفي العام ٢٠١٨م توضح تقديرات صندوق النقد الدولي للتكلفة الناتجة عن الهجمات السيبرانية في القطاعات المالية من واقع الخسائر المحققة جراء هجمات فعلية في ٥٠ دولة حول العالم أن متوسط الخسائر السنوية المحتملة من الهجمات السيبرانية قد يكون كبيراً بما يقدر بنحو ٩٪ من صافي دخل البنوك على مستوى العالم (صندوق النقد العربي،٢٠١٩، ص ١)، ووصولاً إلى العام ٢٠٢٤م في الاتحاد الروسي على سبيل المثال يشير أحدث تقرير سنوي لوزارة الشؤون الداخلية جمعت من خلاله تصنيفاً للمناطق التي لديها أعلى مستوى من الجريمة السيبرانية أوضحت فيه أن الجرائم المكتشفة في العام ٢٠٢٤م باستخدام البطائق البنكية البلاستيكية تخطت ١١٥ ألف حالة وهذا أقل بنسبة ١٣,١٪ مقارنة بالعام ٢٠٢٣م وأن الاحتيال الإلكتروني شكل ٤٠٪ من بين جميع الجرائم السيبرانية في العام ٢٠٢٤م، وأشار التقرير إلى أن الأضرار المالية الناجمة عن الجرائم السيبرانية بشكل عام خلال الخمس السنوات الماضية بلغت حوالي ٥٠٠ مليار روبل بينما وصل المبلغ في العام ٢٠٢٣م ١٥٦ مليار روبل فقط (TADVISER,**24.01.2025**، https://www.tadviser.ru).

المشكلة الأكثر تعقيداً بالنسبة للقطاع المالي والمصرفي في العالم السيبراني الذي لا سيطرة مطلقة فيه لأحد هي إقحام تلك الكيانات المالية في الصراعات الدولية خاصة بعد أن اعتمدتها بعض الدول للإضرار بمصالح الدول المعادية بعدة طرق، سواء بدعم

مجموعات الهاكرز أو توفير الملاذات الآمنة لهم أو شن هجمات سيبرانية على القطاعات الاقتصادية والحيوية بهدف إرباكها واستنزافها وتكبيدها خسائر مالية كبيرة دون أن تدخل معها في حرب مباشرة، ومع استمرار التطور التقني والتكنولوجي تستمر صور الجرائم المالية الإلكترونية باتخاذ أشكال وأنماط جديدة ومتنوعة على مستوى العالم والتي منها:

١. **العمليات المالية الاحتيالية:** أحد أشهر الأمثلة على العمليات المالية الاحتيالية كانت في العام ٢٠١٦م عندما تعرضت لها جمعية الاتصالات المالية العالمية بين البنوك SWIFT وهي الشبكة التي تستخدمها المؤسسات المالية لإرسال واستقبال معلومات وبيانات المعاملات البنكية لسلسلة من الهجمات أدت إلى سرقة ملايين الدولارات وأسفر الهجوم الأول المبلغ عنه والذي وقع في فبراير ٢٠١٦م عن سرقة ٨١ مليون دولار من البنك المركزي في بنغلاديش حيث تمكن المتسللون من استغلال ثغرة في شبكة SWIFT مستخدمين بيانات اعتماد موظفي البنك المركزي في بنغلاديش لإرسال طلبات تحويل أموال احتيالية إلى البنك الاحتياطي الفيدرالي في مدينة نيويورك الأمريكية مطالبين البنك بتحويل الأموال من البنك المركزي في بنغلاديش إلى حسابات في جميع أنحاء منطقة شرق آسيا (Rewired Cybersecurity Governance، 2019، P.97).

٢. **التصيد الاحتيالي** Phishing **لسرقة الأموال من الحسابات البنكية:** وهو نوع من الهجمات التي تهدف إلى سرقة المعلومات الحساسة وهويات المودعين وبياناتهم الشخصية مثل كلمات المرور وأرقام الحسابات والبطاقات البنكية وغيرها من البيانات وقد تتخذ طرقاً متعددة كرسائل البريد الإلكتروني أو الرسائل النصية SMS أو التصيد عبر الهاتف Smishing أو التصيد عبر المكالمات الهاتفية (Council of Veterans - Prosecutor's Office of the Ryazan Region, 2019, www.prokrzn.ru)

٣. **البرمجيات الخبيثة:** من أهمها FASTCASH Malware وتستخدم لاختراق أنظمة الدفع والتحكم بأجهزة الصرافات الآلية ATMs وتوجيهها لصرف الأموال دون الحاجة إلى بطاقات مصرفية.

٤. **حصان طروادة:** وهو برنامج ضار يستخدم لاختراق الأنظمة المالية وتنفيذ أوامر برمجية خبيثة على الشبكات المصرفية، Dridex، Cobalt Strike وهي برمجيات

لاختراق أنظمة البنوك الداخلية وتنفيذ عمليات تحويلات مالية، فيروس الفدية WannaCry والذي ضرب هذا الفيروس أكثر من ١٥٠ دولة في العام ٢٠١٧م ويقوم باختراق أنظمة التشغيل وتشفير بياناتها ثم يعرض رسالة على شاشات حواسيب المؤسسات والكيانات المستهدفة بدفع فدية تكون عادة بالعملات الرقمية المشفرة مقابل فتح التشفير..

ومن أشهر مجموعات القرصنة التي استخدمت تلك البرمجيات الخبيثة لسرقة ملايين الدولارات من المؤسسات المالية حول العالم ECCENTRIC BANDWAGON، ومجموعة Beagle Boyz التي تتهمها الولايات المتحدة الأمريكية أنها تتبع الاستخبارات العسكرية في جمهورية كوريا الشمالية وأنها استولت على ما يقرب من ٢ مليار دولار منذ عام ٢٠١٥م على الأقل وفقاً للتقديرات العامة وأن هجماتها في أكتوبر من العام ٢٠١٨م أدت إلى توقف أحد البنوك في أفريقيا عن استئناف خدمات أجهزة الصراف الآلي أو نقاط البيع العادية لعملائه لمدة شهرين تقريباً بعد محاولة حادثة FAST Cash وأنها غالباً ما تقوم بتثبيت أدوات مدمرة لمكافحة الأدلة الجنائية على شبكات الكمبيوتر للمؤسسات الضحية، بالإضافة إلى ذلك في عام ٢٠١٨م قامت المجموعة بنشر برامج ضارة استهدفت أحد البنوك في تشيلي مما أدى إلى تعطل آلاف أجهزة الكمبيوتر والخوادم لصرف الانتباه عن محاولاتهم إرسال رسائل احتيالية من محطة SWIFT المخترقة الخاصة بالبنك (CISA.GOV، 24.10.2020، www.cisa.gov)،

٥. استهداف التطبيقات والمحافظ الإلكترونية البنكية: Banking Malware: هنالك برمجيات خبيثة كثيرة لعل أشهرها تلك التي تعمل على استهداف التطبيقات والمحافظ الرقمية وتكون مثبتة على أجهزة الضحايا نتيجة تصيد احتيالي أو التحميل من مصادر غير موثوقة أو عن طريق استغلال الثغرات الأمنية وتستمر البرمجيات بمراقبة أنشطة المستخدم خاصة عند الدخول للتطبيقات والمحافظ الرقمية أو حتى المواقع المصرفية ثم تلتقط اسم المستخدم وكلمات المرور التي يدخلها الضحية ثم تلتقط رموز المصادقة الثنائية MFA وتستخدم في سبيل ذلك تقنيات مثل keylogging (تسجيل ضغطات لوحة المفاتيح) أو Scraping (التقاط صور للشاشة) لسرقة MFA التي يتم إرسالها عبر الرسائل النصية ثم تضيف البرامج الضارة المصرفية النظام التحويلي التلقائي ATS لالتقاط رمز MFA وبدء المعاملات وتنفيذ التحويلات المالية , www. Finance personnel, 2023 (,informationsecurity.com.tw) . .

المطلب الثالث
أنظمة الذكاء الاصطناعي

ظهر مصطلح الذكاء الاصطناعي في أربعينيات القرن المنصرم، واستمرت الأبحاث واللجان العلمية في كلا المعسكرين الشرقي والغربي، ومنذ ذلك الحين قامت تلك اللجان بالعمل على تطويره وهو ما أحدث تقدماً ملحوظاً في عدة مجالات، وفي حقبة الثمانينات والتسعينات مر المجال البحثي للذكاء الاصطناعي بفترات من التراجع والتقهقر منها ما يعد اقتصادياً يدور حول التكلفة والجدوى ومنها ما هو سياسي تم صبغة بطابع ديني حتى وصل الأمر في التسعينيات أن أصبح مصطلح الذكاء الاصطناعي من المحرمات تقريباً، بل تم وصفه في اللغة الجامعية بمصطلح أكثر تواضعاً «الحوسبة المتقدمة»(Council of Europe Portal. www.coe.int/en/web/artificial-intelligence)، ومع مطلع الألفية الثالثة كانت الدول الفاعلة في مجال الذكاء الاصطناعي قد امتلكت كميات مهولة من البيانات والمعلومات Big data فظهر الذكاء الاصطناعي بحلة جديدة وإمكانات خارقة خيل فيها للبشرية بأنه علم جديد خرج من رحم تلك الثورة المعلوماتية وهو ما حدا بالباحثين والدارسين والمهتمين في كافة المجالات أن يرفدوه بالدراسات والأبحاث، فمنهم من تناوله من ناحية فلسفية، ومنهم من درسه وفقاً لقواعد علم الاجتماع، ومنهم من نظر إليه من زاوية اقتصادية وسياسية، وهذا يفسر الزيادة الهائلة في المنشورات العلمية الخاصة بالذكاء الاصطناعي التي لم تبدأ إلا في حدود عام ٢٠٠١م، ثم تراجعت نسبة المنشورات العلمية إلى الاختراعات من ٨:١ في عام ٢٠١٠م إلى ٣:١ في عام ٢٠١٦م بما يوحي بالتحول من البحث النظري إلى الاستخدام العلمي لتكنولوجيات الذكاء الاصطناعي في المنتجات والخدمات التجارية والاقتصادية (المنظمة العالمية للملكية الفكرية. ٢٠١٩)، ولقد بات الذكاء الاصطناعي قدراً يحتم على الدول والحكومات خوض غماره والتنافس فيه وعدم تفويت فرص ثمينة هي في أمس الحاجة لها من أجل ضمان دوام بقائها واستمراريتها وتطوير قدراتها وإمكانياتها في شتى المجالات المختلفة، ومما لا شك فيه أن جهود الدول والقوى الفاعلة في الابتكار والتصنيع أوجدت بنى تحتية رقمية رائدة من خلالها تطورت قدرات الذكاء الاصطناعي في جميع المجالات، ويأتي في مقدمتها التحول الجذري الذي أحدثه الذكاء الاصطناعي في مختلف القطاعات العسكرية والأمنية والاقتصادية والصناعية والصحية والتعليمية والخدمات اللوجستية والأمن الغذائي.

ومن خلال التعريفات المختلفة والمتباينة التي اختلفت بحسب المراحل والأطوار التي مر بها حيث تجلى الطور الأول للذكاء الاصطناعي بقدرات برمجية حاسوبية بسيطة تعالج مشاكل محددة، وبمرور الزمن بدأ طور النماذج الأكثر تعقيداً، والتي تعتمد على تقنيات التعلم العميق، بما في ذلك الشبكات العصبونية الصناعية وهو ما سمح للأنظمة بفهم ومعالجة البيانات بشكل أكثر دقة كما أصبحت قادرة على التعلم الآلي من أخطائها والعمل على تصحيحها وتحسينها، ثم ظهر الطور الذي استطاعت فيه تقنيات الذكاء الاصطناعي التفاعل مع محيطها بشكل أوسع وصار بإمكانها التعرف على الأصوات والصور والتفاهم اللغوي وفهم المشاعر ورصد السلوك البشري وتفسيره، وبناء على ذلك فالذكاء الاصطناعي هو «العلم الذي تستخدم فيه تقنيات التكنولوجيا المتطورة مع المخزون المعرفي الإنساني بهدف إكساب الآلة مهارات وقدرات بشرية متخصصة في العالم الافتراضي أو العالم المادي أو فيهما معاً وإمكانية رفدها بخاصية محاكاة البشر في الشخصية والتعلم والعمل والاستقلالية وفي الاستنتاج واتخاذ القرارات والتنفيذ وفقاً للمعطيات والمدخلات التي غذيت بها من قبل صانعها أو مالكيها أو مطوريها».

وأنظمة الذكاء الاصطناعي المستخدمة في كافة المجالات تتكون بشكل أساسي من مجموعة من الركائز والنُهُج وعلى النحو الآتي:

أولاً: ركائز الذكاء الاصطناعي PILLARS OF AI:

جميع أنظمة الذكاء الاصطناعي تتكون من ثلاث ركائز عريضة PILLARS OF AI تعمل جنباً إلى جنب ولا يمكن لها أن تعمل بنجاح دون بناء الأبعاد الثلاثة على بعضها البعض (LaTrelle Annette Bolding. **2023**)، وتتجلى ركائز أنظمة الذكاء الاصطناعي في التالي:

أ. **بنية المجال** Domain Structure: فمن خلال هذا الهيكل يقوم المهندسون وغيرهم من الخبراء بوضع الأطر النظرية وكتابة القواعد التي تعمل على تقسيم المشكلات المعقدة إلى مهام أصغر وأبسط يمكن حلها باستخدام التعلم الآلي، بمعنى أنه لا بد لإنتاج نظام ذكاء اصطناعي يستطيع التعامل مع العالم الحقيقي أن يتم تحديد النظرية ووضع القواعد ذات الصلة، فإذا كنت ترغب في إنشاء نظام لديه القدرة على التواصل مع العملاء على سبيل المثال سيكون عليك تحديد نوايا العملاء ورغباتهم وميولهم بطريقة تسمح بإجراءات تعلم الآلة المختلفة لإنشاء حوار بين النظام

والعملاء(Matt Taddy. 2019.P. 63-65).

ب. **توليد البيانات** Data Generation: تنقسم البيانات إلى فئتين: الفئة الأولى من البيانات تعتبر المواد الخام والأصول ذات الحجم الثابت لأي نظام ذكاء اصطناعي ويتم استخدامها لتدريب ذلك النظام على المهام العامة، أما الفئة الثانية من البيانات هي التي يتم إنشاؤها وتوليدها بشكل نشط عن طريق النظام أثناء اختبار الأداء وتطويره بتلك الطريقة «توليد البيانات» وتدفقها المستمر يسمح بتغذية خوارزميات التعلم بالمعلومات الجديدة والمفيدة، ويمكن تقسيم البيانات الضخمة إلى فئتين عريضتين: البصمات الرقمية التي يولدها الإنسان وبيانات الآلة، ومع استمرار نمو تفاعلاتنا على الإنترنت تستمر بصماتنا الرقمية في التزايد على الرغم من أننا نتفاعل بشكل يومي مع الأنظمة الرقمية إلا أن معظم الناس لا يدركون مقدار المعلومات التي تتركها حتى النقرات أو التفاعلات التافهة- فبحلول فبراير ٢٠١٣م كان لدى «فيسبوك» أكثر من مليار مستخدم منهم ٦١٨ مليون مستخدم نشط يومياً، لقد شاركوا ٢,٥ مليار عنصر وأعجبوا بـ ٢,٧ مليار أخرى كل يوم مما أدى إلى توليد أكثر من «٥٠٠» تيرا بايت (خمسمائة ألف جيجا بايت) من البيانات والمعلومات الجديدة على أساس يومي، وفي مارس من نفس العام كان موقع «لينكد إن» Linkedin وهو موقع للتواصل الاجتماعي موجه للأعمال يضم أكثر من ٢٠٠ مليون عضو فيه وينمو بمعدل عضوين جديدين كل ثانية مما أدى إلى توليد ٥,٦ مليار عملية بحث موجهة بشكل احترافي (Marc Dugain، Christophe Labbé. 2016).

ج. **التعلم الآلي** Machine Learning: يعتبر «التعلم الآلي» الركيزة الثالثة التي تقوم عليها أنظمة الذكاء الاصطناعي، فمن خلال البيانات الضخمة Big Data التي تنشئها الركيزة الثانية باستمرار والتي يتم تخزينها على أجهزة خصصت لذلك يتم معالجة تلك البيانات باستخدام (خوارزميات) مبرمجة لأداء المهام التحليلية بمهارة ومن خلالها يمكن للآلة التعرف على الأنماط المستهدفة للتنبؤ بالنتائج المستقبلية والتعلم من خلال التجربة، ويعرف «التعلم الآلي» ML بأنه عبارة عن مجموعة فرعية من الذكاء الاصطناعي تركز على تمكين الآلات من التعلم من البيانات وتحسين أدائها دون برمجتها بشكل صريح وتستخدم تعلم الآلة تقنيات إحصائية لتحليل وتفسير الأنماط في البيانات مما يمكن الآلات من إجراء تنبؤات أو تصنيف المعلومات أو اكتشاف الرؤى المخفية والخروج باستنتاجات مشمولة بقرارات قابلة

للتنفيذ آلياً دون تدخل بشري (Jasper Blackwell. 2023. P. 4).

ثانيًا: نُهُج الذكاء الاصطناعي AI Approach:

لا يقتصر الأمر في بناء نماذج الذكاء الاصطناعي على الركائز فحسب، وإنما هنالك أيضاً استراتيجيات أو نهج أساسية تعتمد عليها أنظمة الذكاء الاصطناعي ويتم استخدامها وفقاً لطبيعة المجالات والأهداف والغايات الوظيفية المختلفة المراد تحقيقها وتتمثل في التالي:

أ. **نظرية العقل** Theory of Mind: يُعْنى نهج «نظرية العقل» بأهمية فهم التفكير والإدراك البشري وكيف يمكن تكراره في الآلات عن طريق محاكاة عمليات وسلوكيات تفكير البشر في الإدراك والاستدلالات وحل المشكلات، ومن ثم فإن تلك التقنيات ستقوم وفقاً لنظرية «النهج العقلي» بفهم نوايا ومعتقدات ورغبات وعواطف البشر والتنبؤ بسلوكياتهم والتفاعل معهم بشكل إيجابي.

ب. **الآلات التفاعلية** Reactive Machines: تم استخدام نهج «الآلات التفاعلية» في تصميم أقدم نماذج الذكاء الاصطناعي ويعتبر جهاز الكمبيوتر Deep Blue من شركة IBM الذي هزم الروسي «غاري كاسباروف» Garry Kasparov بطل العالم في الشطرنج في شهر مايو من العام ١٩٩٧م أحد النماذج الشهيرة للآلات التفاعلية، حيث تدرك ما حولها بشكل مباشر وتتصرف بناء على ما تراه وليس بإمكانها التعلم أو تصور الماضي أو المستقبل وهو ما يعني أن قدراتها لمحاكاة الذكاء البشري محدودة.

ج. **الذاكرة المحدودة:** الذكاء الاصطناعي ذو الذاكرة المحدودة أكثر تقدماً وتعقيداً من الآلات التفاعلية من حيث القدرة على تخزين واستخدام المعلومات وتحسين أدائها باستمرار، وهذا مشابه لكيفية عمل الدماغ البشري الذي يتعلم ويتكيف، حيث تستخدم نماذج الذكاء الاصطناعي البيانات التي تخزنها الذاكرة المحدودة لإنشاء الأطر التي تساعده على اتخاذ القرارات (Victor Singh، 2023، P.42).

د. **الوعي الذاتي** Self-Awarness: يعتبر نهج «الوعي الذاتي» امتداداً لنهج نظرية «العقل» ولكن ببعد أكثر عمقاً وشمولاً والهدف منه استخدامه في تصميم نماذج ذكية لديها القدرة على تشكيل وعي وإدراك ذاتي يسمح لها بتقييم حالتها الداخلية وقدراتها وفهم كينونتها باعتبارها كائناً مستقلاً عن الكيانات الأخرى يمثل ذاته دون

استخدام الوعي البشري كنموذج لها، وقد انقسم كثير من العلماء والباحثين ورواد التكنولوجيا حوله بين من يدق ناقوس الخطر ويثير القلق والرعب في نفوس الناس مؤكداً أن نماذج الذكاء الاصطناعي الواعية بذاتها باتت واقعاً ملموساً وأنها الآن في مرحلة تفوق ذكاء وقدرات البشر وقد باتت قريبة جداً من مرحلة التفرد الذاتي وما يخشونه هو ما وراء ذلك التفرد الذي قد يؤدي إلى أن تتحكم بالبشر أو قد تتسبب بكوارث وأضرار للحضارة البشرية أو ترسم نهايتها، وبين من يعتبر «الوعي الذاتي» مجرد نظرية لم تتحقق بعد وأنه سيتم إنتاج نماذج للذكاء الاصطناعي واعية لذاتها بحلول عقد أو عقدين من الزمن تظهر قدرات متقدمة في مجالات محددة إلا أنها لن تمتلك نفس الوعي الذاتي للبشر، بل إن هنالك من ذهب إلى أبعد من ذلك بكثير وبأسلوب فلسفي عميق.

المطلب الرابع
أنظمة الذكاء الاصطناعي وتعزيز أدلة الإثبات في الجرائم المالية الإلكترونية

قبل الحديث عن دور أنظمة الذكاء الاصطناعي في تعزيز أدلة الإثبات الجنائي في شأن الجرائم المالية الإلكترونية، لا بد من الإشارة إلى أن الذكاء الاصطناعي قد أحدث ثورة عارمة في المجال الاقتصادي أدت إلى مراجعة النظريات والمسلمات والمفاهيم الاقتصادية التي كانت قد ترسخت واستقرت منذ زمن وخلق بعداً جديداً لاقتصاديات الدول وأعاد تشكيل الأسواق العالمية، ولكنه أوجد أيضاً مخاطر أثرت سلباً على عالم المال والأعمال، فعلاوة على استخدام العصابات الإجرامية الاقتصادية الدولية التزييف العميق لتنفيذ أنشطة احتيال للإضرار بالتجارة الإلكترونية العالمية عن طريق تحديد نقاط الضعف في النظام المالي، واستخدامها في التلاعب بالبيانات وغسيل الأموال وتمويل الأنشطة غير المشروعة عبر الإنترنت باستخدام التقنيات الناشئة، مثل منصات الدفع الجديدة والعملات المشفرة لإجراء معاملات معقدة ومتعددة الطبقات يصعب اكتشافها وتتبعها، هنالك أيضاً الأنظمة الذكية المالية المستقلة التي تستخدم لاتخاذ قرارات بشأن التداولات في الأسواق المالية العالمية حيث يمكن لتلك الأنظمة اكتشاف الأنماط والاتجاهات في السوق واتخاذ قرارات التداول بشكل أسرع وأكثر دقة غير أن المخاطر التي يمكن أن تتسبب بها قد تؤدي إلى تحيزات خوارزمية في اتخاذ القرارات أو انهيارات في الأسواق المالية أو حتى الكساد الاقتصادي، ويشير كثير من المتخصصين أن هنالك ستة مخاطر رئيسية قد تسببها الخدمات المالية التي تعتمد على الذكاء الاصطناعي: المخاطر الأخلاقية والخصوصية، وتقلبات السوق، وقضايا التلاعب بالأسعار، بالإضافة إلى مخاطر الاستعانة بمصادر خارجية مركزية، واتخاذ القرارات بطريقة الصندوق الأسود، ويمكن أن تكون هذه المخاطر الستة الكبرى بحسب خصائصها والأشياء المتضررة منها، وقد تم تصنيفها إلى ثلاثة مجالات رئيسية، الأول: هو التأثير على الأفراد المشاركين في السوق وهي القضايا الأخلاقية والخصوصية، والثاني: هو التأثير على السوق بشكل عام، أما الثالث: فتأثير السوق، أي تقلبات السوق وقضايا التلاعب بالأسعار وهو يركز على الضرر الذي يلحق بالمؤسسات المشاركة والأشخاص الاعتباريين، كما أن هنالك مخاطر تقنية بحته وتشمل المخاطر الفنية والتركيز على الاستعانة بمصادر خارجية وغموض عملية صنع القرار (Xie Minghua, Li Zhenhua, date unknown, page46).

وبالعودة إلى أنظمة الذكاء الاصطناعي ودورها في تعزيز أدلة الإثبات الجنائية في الطب الشرعي الرقمي فإن تقنيات وأنظمة الذكاء الاصطناعي تلعب دوراً حاسماً ومهماً في تسريع وتعزيز وتحسين كفاءة أعمال التحقيق في الجرائم السيبرانية بشكل عام، وفي شأن الجرائم المالية الإلكترونية فقد مكنت تقنيات وأنظمة الذكاء الاصطناعي محللي الطب الشرعي الرقمي، وسلطات إنفاذ القانون من استخراج المعلومات ذات الصلة بالجرائم المالية الإلكترونية، واكتشاف الملفات المحذوفة أو المخفية، واستعادتها وفك التشفير، وإعادة بناء الأحداث ومحاكاتها باستخدام الأدلة الرقمية لفهمها، وتحليلها للوصول إلى إثباتها أو دحضها، ولقد أدى التكامل المتزايد للذكاء الاصطناعي وخوارزميات التعلم الآلي لإحداث تغييرات كبيرة في مجال الطب الشرعي الرقمي لتحقيق تحليل أسرع وأكثر دقة للبيانات، ومعالجة كميات كبيرة من البيانات في وقت قياسي، وتحديد الأنماط وتحليل الأدلة الرقمية، واكتشاف الحالات الشاذة والتعرف على الهويات بطرق كانت تعتبر مستحيلة في السابق (Global Growth Insights.2023. www.globalgrowthinsights.com)، وأصبح بإمكان نماذج التعلم الآلي التمييز بين المعاملات المشروعة وغير المشروعة بناء على سلوك المستخدمين وتاريخهم المالي، وبما أن المجرمين الماليين يتواصلون بشكل متكرر من خلال القنوات الرقمية تاركين وراءهم ثروة من البيانات النصية التي يمكن أن تكون بمثابة كنز من الأدلة يستخدم المحققون خوارزميات معالجة اللغة الطبيعية NLP للكشف عن الروابط الخفية والأنشطة غير القانونية والنوايا السيئة حيث تسمح قدرة البرمجة اللغوية العصبية على تحليل وفهم اللغة البشرية في المؤسسات المالية وتلعب دوراً فعالاً في غربلة هذه البيانات النصية، وعمل مسح لرسائل البريد الإلكتروني وسجلات الدردشة والرسائل الأخرى لتحديد المحادثات المشبوهة أو المدانة (FDM. 2023. www.fdmgroup.com)، كما أن هنالك تقنيات أخرى تقوم بتحليل حركة المرور على الشبكات في المؤسسات المالية والمصرفية، والتقاط وتحليل الحزم المنقولة عبر الشبكة وتسجيلها وتحليل تدفق البيانات والسجلات في أجهزة الشبكة المختلفة وربط الأدلة ببعضها، ما يؤدي إلى تحديد آثار البرامج الضارة والتطبيقات غير المصرح بها أو تسريبات البيانات...إلخ.

الخاتمة والتوصيات

التطور التكنولوجي والتقني وظهور الاقتصاد الرقمي مثل رافداً حيوياً للدول والحكومات هي في أمس الحاجة إليه من أجل ضمان دوام بقائها واستمراريتها وتطوير قدراتها وإمكانياتها، ولقد أدى الابتكار في الصناعة المالية والتحول الرقمي في هذا المجال إلى خلق بنية تحتية رقمية رائدة وظهور منصات تعتمد عليها الخدمات المصرفية الرقمية والمعاملات المالية عبر الإنترنت فأوجدت بذلك فرصاً ثمينة، واستثمارات جديدة ولكنها جلبت معها أيضاً مخاطر وتحديات حديثة ومبتكرة أضرت بالدول والحكومات وكبدتها خسائر اقتصادية واجتماعية، وفي هذا المضمار الجديد كان ولازال التنافس والصراع على أشده بين عالم الجريمة في الشبكة المعلوماتية من جهة وبين الكيانات الاقتصادية والمالية، وإلى جانبها سلطات العدالة الجنائية وإنفاذ القانون، ومع ذلك فإن الواقع العملي يثبت أن ميزان العدالة لا زال مختلاً ويميل دائماً لكفة المتفوق في المجال التقني والتكنولوجي، وبينما تشير التقارير العامة إلى أن تقنيات الذكاء الاصطناعي في مجال تعزيز أدلة الإثبات في القضايا المالية الإلكترونية قد حققت قفزات نوعية مثمرة، إلا أن كثيراً من الدول المتأخرة في هذا المجال لا زالت تعتمد على أدوات معرفية ضحلة على كافة الأصعدة القانونية والأمنية والأكاديمية والتقنية، ولعل ذلك يرجع إلى سيطرة القوى الفاعلة في مجال الذكاء الاصطناعي خارطة البحوث الدولية والاحتكارية الجشعة التي تمارسها كبريات الشركات التكنولوجية والشركات الناشئة في هذا المجال وأغلبها غربية بامتياز، غير أن الواقع العالمي الجديد في كافة المجالات بشكل عام وفي مجال المال والأعمال على وجه الخصوص قد أجبر الدول النامية لخوض غمار التحول الرقمي دون استراتيجيات فاعلة أو رؤى واضحة، وهو ما أدى إلى ظهور الكثير من النسخ الرديئة الوصولية والانتهازية التي اقتحمت مجال الذكاء الاصطناعي والأمن السيبراني في كافة التخصصات والمجالات لجني الأموال الكثيرة مدعومة بأصحاب النفوذ والمحسوبية، مستغلة حاجة وضعف كثير من الدول والحكومات في هذا المعترك العصري والمستقبلي المهم، ولكنها سرعان ما أثبتت فشلها في أول اختبار عملي في كثير من الدول، ومن ثم فإنه يجب على صناع القرار التنبه لذلك ما لم فإن المخرجات والنتائج ستكون كارثية على تلك الدول وتلكم الحكومات.

وفي بلادنا وبرغم الظروف الاستثنائية التي تمر بها إلا أن التحول الرقمي قد أحدث تغييرات عميقة في السياسات العامة للدولة وفي الوعي المجتمعي وفي أغلب المجالات

بشكل عام وفي قطاع المال والأعمال على وجه الخصوص، ولقد كان لقطاع الاتصالات والبنوك في بلادنا دوراً رائداً ومحورياً في دفع عجلة التحول الرقمي وتحسين الخدمات وزيادة الفرص الاستثمارية رغم تواضعها، وفي تشكيل وعي جديد لدى مؤسسات صناعة القرار، ومع ذلك لا زالت التحديات في هذا المجال كبيرة وتستدعي تضافر جهود كل أطراف المصلحة في العالم الافتراضي لتبني استراتيجيات فاعلة وناجعة للتصدي لتلك المخاطر، وفيما يلي بعض التوصيات والمقترحات بشكل عام، وعلى النحو التالي:

١. لا بد أن يتم تطوير سياسات الدولة الجنائية وتشريعاتها الوطنية بما يتلاءم مع الطبيعة الخاصة للجرائم السيبرانية وتبني استراتيجيات فعالة في مواجهتها وإشراك القطاع الخاص وبقية أطراف المصلحة في رسم تلك السياسات والاستراتيجيات وتوزيع المسؤوليات بشكل مرن وفعال.

٢. للقطاع الخاص دور كبير وفعال في العالم السيبراني وفي المجال التكنولوجي والتقني وصار لاعباً فاعلاً ومؤثراً لابد من الاستفادة منه وتمكينه وتذليل الصعوبات ليقوم بدوره الإيجابي والبناء على أكمل وجه.

٣. من الأولويات الملحة تأهيل سلطات إنفاذ القانون وبناء قدرات رجال العدالة الجنائية للتصدي للأنشطة الإجرامية السيبرانية حتى لا نكون أمام ما يمكن أن نسميه بأمية رجال العدالة الجنائية وإنفاذ القانون تجاه جرائم العالم السيبراني.

٤. ينبغي الاستثمار في توعية المجتمع بالجرائم الإلكترونية من أجل معالجة مشكلة انخفاض معدلات الإبلاغ عن الجريمة الإلكترونية مقارنة بالجرائم الأخرى.

٥. يجب الاستفادة من كل تجارب الدول في مجال الأمن السيبراني ومكافحة الجرائم الإلكترونية وعدم تكرار الأخطاء التي وقعوا فيها والبدء من حيث انتهى الآخرون واستبعاد النسخ الرديئة في هذا المجال.

٦. في شأن التعاون الدولي لا بد من التروي قبل الانضمام أو المصادقة على أي اتفاقية متعددة الأطراف، وما يجب فعله في الوقت الحالي هو عقد الاتفاقات الثنائية مع الدول الصديقة فقط، والاستفادة من تجاربها وإمكانياتها من خلال تدريب الكوادر ونقل الخبرات والتعاون والتنسيق في

مجال الأمن السيبراني ومكافحة الجرائم الإلكترونية.

٧. معيار نجاح أعمال حوكمة رشيدة للعالم السيبراني مرهون بتضافر الجهود للعمل بروح الفريق لمناقشة أهم القضايا المتعلقة بالسياسات العامة لحوكمة العالم السيبراني بمفهومه القائم على الأسس والقواعد والطرق العلمية والمنهجية من أجل خلق توازن بناء تتحدد فيه أدوار ومسئوليات الجهات ذات العلاقة بغية تعزيز واستدامة ومتانة وأمن واستقرار وتطوير هذا العالم وبما يراعي مصالح كل الأطراف أصحاب المصلحة باعتبار تلك الجهود هي المداميك المتينة والأرضية الصلبة التي ترتكز عليها أي سياسة جنائية ناجعة وفعالة لمواجهة ومكافحة الجرائم الإلكترونية.

٨. الإسراع في إعادة تشكيل لجان جديدة قائمة على الكفاءات النوعية والمتخصصة لمراجعة مشروع القانون الذي أعدته وزارة الاتصالات وتقنية المعلومات وإشراك بقية أطراف المصلحة في بلادنا للخروج برؤية مشتركة تسرع من إصدار قانون خاص بتلك الجرائم.

٩. إنشاء هيئة وطنية للأمن السيبراني ومكافحة الجرائم الإلكترونية تضم نخبة من الكفاءات النوعية المتخصصة من كل الجهات ذات العلاقة والعمل بروح الفريق الواحد، مالم فإن أي سياسة جنائية لمواجهة تلك الجرائم محكوم عليها بالفشل.

١٠. إنشاء شعبة متخصصة بالأمن السيبراني والجرائم الإلكترونية في السلطة القضائية ورفدها بمعمل جنائي خاص بالأدلة الإلكترونية وتوفير الإمكانيات اللازمة لتمكينها من العمل.

١١. لابد للمؤسسات المالية والمصرفية تبني استراتيجيات فاعلة لحماية أنظمتها والاستعانة بتقنيات الذكاء الاصطناعي لمساعدتها في التصدي للجرائم المالية الإلكترونية والتعاون مع سلطات إنفاذ القانون وعقد ورش تدريبية معها.

١٢. لا بد من وضع لوائح وتنظيمات صارمة لشركات الأمن السيبراني وشركات الحوسبة السحابية وغيرها من الشركات العاملة في هذا المجال، وضرورة توافق خوارزمياتها وأنظمتها مع معتقدات وقيم وعادات وأعراف وقوانين الدولة اليمينة وإنشاء لجان دورية لمراقبة ضمان الجودة والكفاءة وكذا ضمان عدم مشاركات

أطراف أخرى للبيانات الوطنية، وأخيراً مراقبة الجودة في العملية التعليمية والبحثية الأكاديمية كي لا تقع بلادنا ضحية للنسخ الرديئة التي كبدتنا أضراراً فادحة طالت كافة المستويات في الدولة.

قائمة المراجع

- صندوق النقد العربي. "الأمن السيبراني في القطاع المصرفي". موجز سياسات. العدد ٤، أبوظبي: يونيو ٢٠١٩م.
- تشانغ جيو فنغ، شياو سا، تشانغ جيفنغ. دراسة حول القضايا الرئيسية المتعلقة بالجرائم المالية عبر الإنترنت. مركز أبحاث القانون المالي بجامعة بكين. العدد ٨٩، ٢٠١٤ – إصدار خاص حول التمويل والقانون عبر الإنترنت. (مرجع صينيـــ باللغة الصينية المبسطة Simplified المستخدمة في البر الصيني).

معهد تشونج لون للأبحاث. الابتكار المالي: تحليل النماذج والقضايا القانونية المعقدةـ النماذج والحلول القانونية. دار النشر القانونية. تاريخ النشر: مايو ٢٠١٨. (مرجع صيني– باللغة الصينية المبسطة Simplified المستخدمة في البر الصيني).

- Zhang Jiufeng, Xiao Sa, Zhang Jifeng, 'Discussion on Key Issues of Internet Financial Crimes,' Peking University Financial Law Research Center, 2014, Issue 89 — Special Issue on Internet Finance and Law

  Zhonglun Research Institute, 'Financial Innovation: Analysis of Models and Difficult Legal Issues, Models and Legal Solutions,' Law Press, Publication Date: May 2018.

- مؤسسة إنتر كرايم برس للطباعة والنشر. كل شيء عن المال: الجرائم المالية باستخدام الإنترنت. أخبار. أوراق نقدية حول العالم.٢٠٠٦. ٠٤٢٥.، تمت المشاهدة في: ٢٠٢٥,٠١,٢٢،)موقع إلكتروني باللغة الروسية).

- InterCrime-press: all about money, Financial crimes using the Internet, News, Banknotes of the countries of the world, 25.04.2006, Date viewed: 22.01.2025, at: https://www.icpress.ru/news/19915/.

- موقع إخباري متخصص TADVISER. عدد الجرائم الإلكترونية في روسيا. الجرائم الإلكترونية والصراعات السيبرانية: روسيا. ٢٠٢٥,٠١,٢٥، تاريخ المشاهدة: ٢٠٢٥,٠٢,٠٤، في:)موقع إلكتروني باللغة الروسية).

- TADVISER, Number of Cybercrimes in Russia, Cybercrime and Cyberconflicts: Russia, 25.01.2025, Accessed: 04.02.2025, at: https://www.tadviser.ru/index.php/Article:Number-of-Cybercrimes-in-Russia

Valeria San Juan & Aaron Martin. Cyber Governance and the Financial Services Sector-The Role of Public-Private Partnerships. Rewired Cybersecurity Governance. First Edition. Edited by: Ryan Ellis & Vivek Mohan. 2019 John & Wiley Sons, Inc.

- مجلس المحاربين القدامى بمكتب المدعي العام لمنطقة ريازان. المسؤولية الجنائية عن ارتكاب الاحتيال باستخدام الإنترنت والاتصالات المحمولة. متابعات. ٢٩ أغسطس ٢٠١٩، تمت المشاهدة في: ٢٠٢٥/٠٥/٠٢، في:)موقع إلكتروني باللغة الروسية(.

- http://www.prokrzn.ru/active/comments/vopros-otvet/ugolovnaya-otvetstvennost-za-sovershenie-moshennichestv-s-ispolzovaniem-seti-internet-i-sotovoy-svya/.

- Veterans Council - Prosecutor's Office of the Ryazan Region, Criminal liability for committing fraud using the Internet and mobile communications, ACTIVITY, August 29, 2019, Date accessed: 05.02.2025, at: http://www.prokrzn.ru/active/comments/vopros-otvet/ugolovnaya-otvetstvennost-za-sovershenie-moshennichestv-s-ispolzovaniem-seti-internet-i-sotovoy-svya/.

- CISA, FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks. CYBERSECURITY ADVISORY.CYBERSECURITY INFRASTUCTURE SECURITY AGENCY,AN OFFICIAL WEBSITE OF THE US GOVERNMENT, October 24, 2020, Seen in: 09.02.2025, in: https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-239a.

- الموقع الإلكتروني لموظفي الشؤون المالية. أبرز ١٠ برامج خبيثة ناشئة في مجال الخدمات المصرفية عبر الهاتف المحمول في عام ٢٠٢٣. وجهة نظر. هيئة التحرير. ١٨,١٢,٢٠٢٣. متاح على: تم الاسترجاع في ٢٠٢٣/١٢/١٣، في: (موقع تايواني، باللغة الصينية التقليدية Traditional المستخدمة في تايوان وهونج كونج).

Financial personnel. 2023 - Top Ten Emerging Mobile Banking Malware. Perspectives. Editorial Department. 2023.12.18. Seen at: Retrieval date: 12.02.2025. At

https://www.informationsecurity.com.tw/article/article-detail.aspx?aid=10864.

Council of Europe Portal. History of Artificial Intelligence. Official Website of

the Council of Europe Portal. Seen on August 25, 2023.
https://www.coe.int/en/web/artificial-intelligence/history-of-ai

- المنظمة العالمية للملكية الفكرية. الاتجاهات التكنولوجية للويبو ٢٠١٩- الذكاء الاصطناعي. WIPO Press, ٢٠١٩.

- LaTrelle Annette Bolding. Institutional Pressures on the Oil and Gas Industry: The Role of Machine Learning,Handbook of Research on Machine Learning- Enabled lot for Smart Applictions Across Industries". IGI Global Publisher of TIMELY KNOWLEDGE. USA. 2023.
- Marc Dugain, Christophe Labbé. L'homme nu La dictature invisible du numérique. Editions Plon, Paris, France, 2016.
- Jasper Blackwell. Unlocking the Power of AI: Navigating the Frontier of Artificial Intelligence. Book acdemy, eBook. 2023.
- Victor Singh. Unleashing AI: a partner, a deferent or a confining force?. published by Victor Singh. 2023.

- شيه مينغهوا، لي تشنهوا. تقرير خاص حول منع ستة مخاطر رئيسية للذكاء الاصطناعي في الخدمات المالية. جامعة تشنغتشي الوطنية. وشركة المعلومات المالية المحدودة. تايوان. بدون تاريخ.

- Xie Minghua, Li Zhenhua, Special Report on Six Major Risks That Financial Services May Trigger in Artificial Intelligence, National Chengchi University, Financial Information Co., Ltd., Taiwan, date unknown.
- FDM. How to Use AI to Fight Financial Crime. Preeta Ghoshal. INSIGHTS FOR ORGANISATIONS. 06.09.2023. Seen in 12.02.2025. in:

https://www.fdmgroup.com/news-insights/ai-in-financial-crime/

- رؤى النمو العالمي. سوق تكنولوجيا الطب الشرعي. المعلومات والتكنولوجيا. ٥ أكتوبر ٢٠٢٣. شوهد في: ١٣,٠٢,٢٠٢٥. (موقع صيني ــ باللغة الصينية المبسطة Simplified المستخدمة في البر الصيني).

- Global Growth Insights. Forensic Technology Market. Information and Technology. October 5, 2023. Retrieved: 13.02.2025. In:
https://www.globalgrowthinsights.com/zh/market-reports/forensic-technology-market-100224/.