مجلة
البحوث والدراسات القضائية والقانونية

معوقات تطبيق الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية في اليمن

الدكتورة / صبرين صالح محمد يحيى

الأستاذ المساعد في المعهد العالي للقضاء اليمني

قال تعالى:

﴿سَيُصِيبُ الَّذِينَ أَجْرَمُوا صَغَارٌ عِنْدَ اللَّهِ وَعَذَابٌ شَدِيدٌ بِمَا كَانُوا يَمْكُرُونَ﴾.

[الأنعام:١٢٤]

الملخص:

هدفت الدراسة إلى التعرف على معوقات تطبيق الذكاء الاصطناعي في مواجهة الجرائم الإلكترونية في اليمن، من خلال معرفة مفهوم الذكاء الاصطناعي وتطبيقاته ومجالات استخدامه في مكافحة الجريمة الإلكترونية، كما تم التعرف على مفهوم الجريمة الإلكترونية وخصائصها والصور التي تتخذها، وأظهرت الدراسة عدة نتائج أهمها: وجود معوقات تواجه تطبيق الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية في اليمن تتمثل في:

- ضعف البنية التحتية.
- نقص الكوادر المتخصصة.
- قصور النصوص التشريعية.
- شحة الموارد المالية.
- تحديات الخصوصية.
- التحديات الأخلاقية.
- الهجمات السيبرانية.

وتوصلت الدراسة إلى عدة توصيات أهمها: ضرورة إقرار مشروع قانون مكافحة جرائم تقنية المعلومات، حتى لا يترك الحكم في الجرائم الإلكترونية لتقدير سلطة القاضي، مما يسهل الطعن فيه، وإضافة جزئية خاصة تتعلق بالذكاء الاصطناعي وتطبيقاته، وإنشاء بنية تحتية قوية قائمة على بيانات ضخمة، وتخصيص ميزانية لمواكبة تقنية الذكاء الاصطناعي، مع مراعاة المبادئ الأخلاقية والخصوصية، وتدريب كوادر بشرية لتصميمه واستخدامه قادرة على صد أي هجمات سيبرانية.

مقدمة:

إن التطور الهائل في تكنولوجيا المعلومات والاتصالات في وقتنا الحاضر؛ جعل من العالم قرية صغيرة ربطت الشعوب ببعضها البعض، وزودتها بالعديد من الخدمات والتسهيلات التي تنفذ بأسرع وقت وأقل جهد، وبرزت الكثير من إيجابيات التكنولوجيا في شتى مجالات الحياة، حيث حلت الخدمات الرقمية مكان السجلات والأوراق، وأصبح نشر المعلومات والأخبار عبر الوسائل التقنية لا يأخذ سوى ثوان معدودة، وبالمقابل ظهر العديد من سلبيات التكنولوجيا متمثلة بالجرائم التي تُرتكب في الفضاء الإلكتروني وتعرف بالجرائم الإلكترونية أو المعلوماتية، والتي تتخذ صوراً متعددة منها جريمة الاحتيال والابتزاز والسرقة والتجسس وغيرها من الجرائم التقليدية إلا أن مرتكبيها يستخدمون أساليب وأدوات تقنية حديثة تصعب معها عملية التحقيق والإثبات.

ومع تتالي الثورات الصناعية التي أحدثت طفرة في العالم ابتداءً من المحرك البخاري والفعالية الإنتاجية القصوى ١٧٦٥م، تلتها ثورة الكهرباء والنفط ومحرك الاحتراق الداخلي ١٨٧٠م، ومن ثم ثورة الرقميات وتكنولوجيا المعلومات والإنترنت ١٩٨٩م، وآخرها ثورة الذكاء الاصطناعي وتكنولوجيا النانو ٢٠١٦م، والتي أضحت مؤخراً محط أنظار العالم لما أحدثته هذه الثورة من إعجازات في التكنولوجيا، فصُمم الذكاء الاصطناعي لإنجاز المهام التي يقوم بها البشر، ويؤدي سلوكاً بخصائص تتسم بالطبيعة البشرية التي خص بها الله بني آدم، كالأنماط الذهنية، والتفكير وحل المشكلات، واتخاذ القرارات، وتحليل البيانات؛ للحصول على معلومات دقيقة، والاستنتاج ودراسة الفعل ورد الفعل.

وبناءً على الخصائص التي يتمتع بها الذكاء الاصطناعي، سنسلط الضوء في بحثنا هذا على دوره في مواجهة الجريمة الإلكترونية، والتي انتشرت مؤخراً بشكل كبير في المجتمع اليمني، والتطرق إلى المجالات التي يستخدم فيها الذكاء الاصطناعي لمكافحة هذا النوع من الجرائم، والمتطلبات والاحتياجات اللازمة لتطبيقه، وكذا معرفة التحديات التي تحول دون تطبيقه في بلادنا.

مشكلة البحث:

إن الثورة الشاملة التي أحدثها الذكاء الاصطناعي جعلته يطبق في مختلف التخصصات الاقتصادية والاجتماعية والترفيهية وغيرها، ذلك أن تطبيقاته تتخذ صوراً متعددة يصعب حصرها تدخل في جميع المجالات الإنسانية، بالإضافة إلى المجال الأمني والقضائي وعمليات التجسس على الدول، وقد أدى التطور السريع في أدوات وأساليب

تقنيات الذكاء الاصطناعي في الآونة الأخيرة إلى رفع النمو الاقتصادي والاجتماعي والعسكري في الدول المتقدمة، حيث يقدم حلولاً مبنية على تحليل بيانات ضخمة تساعد في صنع القرارات السليمة، وأصبح العديد من الدول الأجنبية وبعض الدول العربية كالإمارات العربية المتحدة تخصص جزءاً من موازنتها لاستثمارها في تقنيات الذكاء الاصطناعي، وحسب مؤسسة ICD لأبحاث تقنية المعلومات، فقد شهد الاستثمار الإماراتي في تقنية الذكاء الاصطناعي نمواً بنحو (٧٠٪) خلال السنوات الماضية[١]، ومن هذا المنطلق سنحاول في بحثنا هذا معرفة إمكانية الاستفادة القصوى من تقنيات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية التي أرهقت الجهات الأمنية والقضائية في اليمن نتيجة التقدم الحاصل في تكنولوجيا المعلومات والاتصالات، ونحدد مشكلة بحثنا التي تكمن في السؤال الرئيس هو:

ما هي التحديات والمعوقات التي تواجه تطبيق الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية في اليمن؟

ويشتق من السؤال الرئيس الأسئلة الفرعية الآتية:

١. ماهي ماهية الذكاء الاصطناعي، والخصائص التي يتمتع بها، وأنواعه؟
٢. ما هو مفهوم الجرائم الإلكترونية، وخصائصها، وصورها؟
٣. ما هي التحديات والمعوقات التي تواجه استخدام الذكاء الاصطناعي ومواجهة الجريمة الإلكترونية والوقاية منها في اليمن؟

أهداف البحث:

يسعى البحث إلى تحقيق الهدف الرئيس له وهو التعرف على معوقات تطبيق الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية المعاصرة في بلادنا، ويتفرع من هذا الهدف الأهداف الفرعية الآتية:

١. تحديد مفهوم الذكاء الاصطناعي والخصائص التي يتمتع بها، ومتطلباته.
٢. بيان الجرائم الإلكترونية، وخصائصها والصور التي تتخذها.
٣. تسليط الضوء على التحديات والمعوقات التي تواجه تطبيق الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية في اليمن.

(١) الشاعر، سعود عبدالقادر. (٢٠٢٠). دور الذكاء الاصطناعي في تفعيل إجراءات التحقيق الجنائي في الجرائم الالكترونية: دراسة مقارنة. رسالة منشورة كلية القانون، جامعة عجمان، الإمارات العربية المتحدة. ص٨.

أهمية البحث:

تبرز أهمية البحث من خلال أهمية الموضوع والمتغيرات التي ترتكز على دراستها وتحديدها في إطار الأهمية العلمية والأهمية العملية:

الأهمية العلمية:

١. سيسهم البحث في سد فجوة الدراسات المتعلقة بالذكاء الاصطناعي، نظراً لشحة مثل هذه الدراسات في بلادنا.

٢. بناءً على النتائج، سيقدم البحث توصيات متعلقة بدور الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية، تتضمن تطوير السياسات الأمنية والقضائية لحماية الأفراد والمؤسسات من هذه الجريمة.

٣. وتكمن أهمية البحث في تحديد التحديات والمعوقات التي تواجه استخدام الذكاء الاصطناعي في الكشف عن الجريمة الإلكترونية في بلادنا.

الأهمية العملية:

١. يعتبر الذكاء الاصطناعي من الموضوعات الحديثة التي لها آثارها الإيجابية والسلبية على الأفراد والشركات الخاصة والمؤسسات الحكومية، وبالتالي فإنها تستدعي دراستها بعمق.

٢. كما تكمن أهمية البحث في إبراز أهم التحديات والمعوقات التي تواجه تطبيق الذكاء الاصطناعي في الحد من الجرائم الإلكترونية في بلادنا، في ظل تزايد مرتكبيها والآثار التي تخلفها هذه الجرائم على المجتمع اليمني.

٣. ستشكل هذه الدراسة مرجعاً للمشرع اليمني، وذلك في تحديد أهم المعوقات التي تواجه تطبيقات الذكاء الاصطناعي في الحد من الجرائم الإلكترونية في بلادنا.

حدود البحث:

- الحدود الموضوعية: في الموضوع الذي تتناوله وهو التحديات والمعوقات التي تواجه تطبيق الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية المعاصرة في اليمن.
- الحدود المكانية: الجمهورية اليمنية.
- الحدود الزمانية: ١٤٤٧هـ-٢٠٢٥م.

منهج البحث:

تم استخدام المنهج الوصفي التحليلي لمعرفة ماهية الذكاء الاصطناعي وتطبيقاته، ومفهوم الجريمة الإلكترونية، والتحديات المختلفة التي تواجه الأجهزة الأمنية والقضائية في تطبيق الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية في اليمن.

مصادر المعلومات:

تم الاعتماد على مصادر البيانات الثانوية ممثلة بالكتب والمراجع العربية والأجنبية ذات العلاقة، والدوريات والمقالات، والأبحاث والأطر النظرية والدراسات السابقة التي تناولت موضوع البحث، والمطالعة في مواقع الانترنت المختلفة.

أسباب اختيار موضوع البحث:

إن حداثة الموضوع وأهميته وقلة الدراسات المتعلقة بالمعوقات التي تواجه تطبيق الذكاء الاصطناعي في اليمن ودوره في مكافحة الجريمة الإلكترونية، كانت من أهم الأسباب لاختيار موضوع البحث.

تقسيم البحث:

الإطار العام للبحث والدراسات السابقة:

- المطلب الأول: ماهية الذكاء الاصطناعي وأنواعه.
- المطلب الثاني: مفهوم الجرائم الإلكترونية وصورها.
- المطلب الثالث: مجالات وتطبيقات تقنيات الذكاء الاصطناعي في مواجهة الجريمة الإلكترونية.
- المطلب الرابع: تحديات مواجهة الجريمة الإلكترونية بواسطة الذكاء الاصطناعي.
- الخاتمة:
- النتائج.
- التوصيات.

الدراسات السابقة:

تناولت العديد من الرسائل العلمية موضوع البحث، نظراً لحداثة الموضوع وأهميته، وفيما يلي بعض منها:

١. دراسة عبدالمحسن وآخرين. (٢٠٢٥). دور الذكاء الاصطناعي في مكافحة الجريمة باستخدام التقنيات التكنولوجية الحديثة[١].

هدفت الدراسة إلى التعرف على علاقة الذكاء الاصطناعي بالجريمة، وذلك مع زيادة حدوث الجريمة وتهديدها لأمن المجتمع بالذات الجريمة الإلكترونية، وأظهرت الدراسة عدة نتائج أهمها: أنه يمكن لأساليب التحول الرقمي الحديثة أن تمنع الجريمة مستقبلاً، وتوصلت الدراسة إلى عدة توصيات أهمها: وضع أطر تنظيمية تضمن الاستخدام الأمثل للذكاء الاصطناعي في مكافحة الجريمة مع حماية الحقوق والحريات.

٢. دراسة الشهري. (٢٠٢٤). استخدامات تقنيات الذكاء الاصطناعي في مكافحة الجريمة[٢].

هدفت الدراسة إلى التعرف على التقنيات الحديثة المستخدمة في التعرف على بيانات الوجه، التسجيل الصوتي، التعرف على الجناة، وتطبيق التنبؤ الذكي للجريمة قبل وقوعها، وتوصلت الدراسة إلى أن المملكة العربية السعودية تسعى بخطى واثقة نحو استخدام تقنيات الذكاء الاصطناعي بصورة منهجية نظامية، وقد حققت تقدماً في استخدام الذكاء الاصطناعي في المجال الأمني والقضائي، ومن أهم توصيات الدراسة هي: استحداث فروع وأقسام جدية تضمن تقنيات الذكاء الاصطناعي للسيطرة على كافة أشكال الجرائم المعلوماتية.

٣. دراسة قاسم. (٢٠٢٤). دور الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية، دراسة مقارنة[٣].

---

(١) عبدالمحسن، محمد، آل سعد، سعود الشافي والبويدي، بندر عبدالله. (٢٠٢٥). دور الذكاء الاصطناعي في مكافحة الجريمة باستخدام التقنيات التكنولوجية الحديثة. المجلة العلمية، كلية الشريعة والقانون، أسيوط، جامعة الازهر، مصر، ع (٣٧)، (٥١٩-٥٥٩).

(٢) الشهري، البراء جمعان محمد. (٢٠٢٤). استخدامات تقنيات الذكاء الاصطناعي في مكافحة الجريمة. المجلة العربية للنشر العلمي، ع (٦٨)، (٧٣-٩٢).

(٣) قاسم، مراد محمد غالب. (٢٠٢٤). دور الذكاء الاصطناعي في مكافحة الجريمة الالكترونية، دراسة مقارنة. المجلة العصرية للدراسات القانونية، ٢(٢)، (٩٠-١١٤).

هدفت الدراسة إلى التعرف على دور الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية، وموقف الأنظمة العربية منها، وكيف ساهمت السلطات الرقمية وتقنيات التنبؤ بالجرائم في منع وتقليل الجرائم الإلكترونية، وتوصلت الدراسة إلى أن النظامين السعودي والإماراتي عملا على مواكبة التقدم في استخدام الذكاء الاصطناعي بشقيه الصناعي والقانوني، بينما لا يزال النظام اليمني يعتمد على القوانين القديمة في مواجهة الجرائم الإلكترونية، وأوصت الدراسة بضرورة استخدام تقنيات الذكاء الاصطناعي لمواجهة الجرائم الإلكترونية.

٤. دراسة حسن وآخرين. (٢٠٢٤). الطبيعة القانونية للذكاء الاصطناعي، دراسة تحليلية في القانون المدني الليبي[١].

هدفت الدراسة إلى بيان الإطار القانوني والتكييف القانوني لأعمال وتصرفات الذكاء الاصطناعي، ومعرفة الفوارق بين الذكاء البشري وذكاء الآلة وذلك للوصول إلى معرفة أحكام المسئولية التي تحكم الأخطاء الناتجة عنه، وتوصلت الدراسة إلى توافر أهلية خاصة بالذكاء الاصطناعي، ولا يمكن إخضاعه للأحكام العامة للأهلية للشخص الطبيعي أو المعنوي، وتوصلت الدراسة إلى عدة توصيات أهمها: ضرورة إيجاد تشريع خاص بتنظيم المسئولية عن أخطاء الذكاء الاصطناعي الناشئة عن الحوادث.

٥. دراسة الشاعر. (٢٠٢٢). دور الذكاء الاصطناعي في تفعيل إجراءات التحقيق الجنائي في الجرائم الإلكترونية، دراسة مقارنة[٢].

هدفت الدراسة إلى التعرف على دور الذكاء الاصطناعي في تفعيل إجراءات التحقيق الجنائي في الجرائم الإلكترونية، والاستفادة القصوى من تقنيات الذكاء الاصطناعي في كشف الجرائم الإلكترونية، وتوصلت إلى عدة نتائج أهمها: أن هناك مجالات مختلفة للذكاء الاصطناعي في العمل الشرطي والأمني، وهذا غالباً ما يندرج تحت مسمى استراتيجية المدن الذكية، وتوصلت الدراسة إلى عدة توصيات أهمها: ضرورة استخدام

(١) حسن، عفاف عبدالله الحاج وقشوط، أحمد رمضان. (٢٠٢٤). الطبيعة القانونية للذكاء الاصطناعي، دراسة تحليلية في القانون المدني الليبي. المؤتمر العلمي الثاني، لطلاب المرحلة الجامعية والدراسات العليا، الجامعة الأسمرية الإسلامية، ص(١٢٧-١٤٣).

(٢) الشاعر، سعود عبدالقادر. (٢٠٢٠). دور الذكاء الاصطناعي في تفعيل إجراءات التحقيق الجنائي في الجرائم الالكترونية، دراسة مقارنة. رسالة دكتوراه غير منشورة، كلية القانون، جامعة عجمان، الإمارات العربية المتحدة، ص(١-٣٦).

تقنيات الذكاء الاصطناعي التي يتم بواسطتها الحصول على الأدلة المادية في المجال الجنائي للكشف عن الجرائم بشكل عام والجرائم الإلكترونية بشكل خاص.

وتعليقاً على ما سبق من دراسات، فإن الدراسة الحالية تتشابه مع كثير من الدراسات السابقة في المتغيرات والمضمون، وهو كيفية استخدام تقنيات الذكاء الاصطناعي في الكشف عن الجرائم بشكل عام والجرائم الإلكترونية بشكل خاص، وتختلف الدراسة الحالية عن الدراسات السابقة في أنها تبحث عن التحديات التي تحول دون استخدام تقنيات الذكاء الاصطناعي في مواجهة ومكافحة الجرائم الإلكترونية، بالإضافة إلى اختلافها بالحدود المكانية فيما عدا دراسة قاسم(٢٠٢٤) والتي طُبقت في اليمن.

المطلب الأول
ماهية الذكاء الاصطناعي

تمهيد:

إن التطور المتسارع في تقنية المعلومات والاتصالات ودخولها جميع مجالات الحياة، ولأنها أصبحت لغة العصر في زمننا هذا والتي أضحى بمقدورها تقليل الجهد والوقت لتنفيذ جميع الأعمال والمعاملات في شتى المجالات والقطاعات ومنها مجال الجريمة، حيث أظهرت العديد من التطبيقات أبرزها «الذكاء الاصطناعي» الذي حل محل الإنسان في بعض الأعمال، وفي هذا المطلب سنتناول مفهوم الذكاء الاصطناعي والخصائص التي يتمتع بها وأنواعه.

الفرع الأول
مفهوم الذكاء الاصطناعي وخصائصه

يعد مصطلح الذكاء الاصطناعي من المصطلحات الحديثة التي تجذب اهتمام العديد من القراء والباحثين منذ ظهوره، وقد زاد الاهتمام به مؤخراً نتيجة دخوله مجموعة متنوعة من الميادين العلمية والعملية، في كثير من التخصصات الهندسية والطبية والأمنية وغيرها من الميادين، وفي هذا الفرع سنتعرف على مفهوم مصطلح الذكاء الاصطناعي وخصائصه وأهميته.

الذكاء الاصطناعي لغةً:

ذكاء: مصدر ذكي، ذكاء الإنسان، قدرته على الفهم والاستنتاج والحليل والتمييز بقوة فطرته وذكاء خاطره، وذكاء الولد: كان ذكي الفهم، متوقد البصيرة، وذكي عقله: اشتدت فطنته، والذكاء قدرة على التحليل والتركيب والتمييز والاختيار، والتكيف إزاء المواقف المختلفة[1].

ذكاء اصطناعي: قدرة آلة أو جهاز ما على أداء بعض الأنشطة التي تحتاج إلى ذكاء مثل

---

(١) قاموس المعاني الجامع.

https://www.almaany.com//

تاريخ الدخول: ٨/١١/٢٠٢٥م.

الاستدلال الفعلي والإصلاح الذَّاتي[١].

الذكاء الاصطناعي اصطلاحاً:

إن فكرة الذكاء الاصطناعي هي محاكاة العقل البشري في القيام بإنجاز الأعمال الذهنية من خلال تطوير شرائح الكترونية، قادرة على التعلم وتطوير نفسها[٢].

ويعرف الذكاء الاصطناعي بأنه: فرع من فروع الحاسب الآلي يقوم بأداء عدة مهام تحاكي ما يقوم به الإنسان كالسمع والتكلم والحركة والتفكير وغيرها من المهام بأسلوب متقن ومنظم[٣].

كما يعرف بأنه: «الآلات المخترعة بطريقة يدوية تحاكي ذكاء الإنسان»[٤].

وعرف أيضاً الذكاء الاصطناعي بأنه: علم يبحث عن تعريف للذكاء البشري ومحاكاته باستخدام الآلة، فهو يصلح لجميع التوجيهات، فقط يتم تطويره بأساليب برمجة مناسبة لأداء مهام معينة[٥].

وعرفه مارتن ويك أنه «العلم القادر على بناء آلات تؤدي مهام تحتاج للذكاء البشري عند أدائها مثل الاستنتاج المنطقي والتعلم والقدرة على التعديل، كما يمكن أن يعرف على أنه محاكاة بعض جوانب الذكاء البشري من خلل برنامج أو تطبيق محدد»[٦].

ومن خلال التعاريف السابقة يمكننا القول بأن الذكاء الاصطناعي عبارة عن مجموعة من الآلات والشبكات العصبية المبرمجة بطريقة معينة لأداء مهام ذهنية تحاكي المهام التي يؤديها الإنسان.

كما عرفت المفوضية الأوربية الذكاء الاصطناعي بأنه «جملة من الأنظمة تظهر

---

(١) قاموس المعاني الجامع. مرجع سابق.

(٢) الشهري، البراء جمعان محمد. (٢٠٢٤). استخدامات تقنيات الذكاء الاصطناعي في مكافحة الجريمة. المجلة العربية للنشر العلمي، ع(٦٨)، ص٧٦. (٧٣-٩٢).

(٣) الشاعر، سعود عبدالقادر. (٢٠٢٠). دور الذكاء الاصطناعي في تفعيل إجراءات التحقيق الجنائي في الجرائم الالكترونية، دراسة مقارنة. مرجع سابق. ص١٠.

(٤) الأخنش، أمينة والعيداني، محمد. (٢٠٢٣). الذكاء الاصطناعي كآلية لمجابهة الجريمة الالكترونية. مجلة القانون والعلوم البيئية، ع(٢)، ص٥٢٩.

(٥) محمود، ثائر والعطيات، صادق. (٢٠٠٦). مقدمة في الذكاء الاصطناعي. مكتبة المجتمع العربي للنشر والتوزيع، عمان، الأردن، ص١٣.

(٦) سلطاني، خديجة الكبرى. (٢٠٢٥). الذكاء الاصطناعي مداخله ومفاهيمه وأهم خصائصه وتطبيقاته في المعالجة الآلية للغة العربية. مجلة جسور المعرفة، ١١(١)، ص٣١٩.

سلوكاً ذكياً من خلال تحليل بيئتها واتخاذ الإجراءات إما عن طريق برامج أو من خلال أنظمة التعرف على الكلام والوجه وغيرها من النظم»[١].

الذكاء الاصطناعي إجرائياً:

يمكننا تعريف مصطلح الذكاء الاصطناعي المتعلق بموضوع البحث بأنه مجموعة من السلوكيات التي تتمتع بها الأجهزة والآلات المستخدمة في التنبؤ عن الجريمة أو الكشف عنها، والتي تعتمد على بيانات ضخمة وتراكم معرفي من الأساليب المستخدمة في الجرائم الإلكترونية لمواجهتها والوقاية منها.

ويتميز الذكاء الاصطناعي بعدة خصائص، وهي:

١. القدرة على التنبؤ:

يحتوي الذكاء الاصطناعي على بيانات ومعلومات وخوارزميات وخبرات تراكمية تمكنه من استرجاعها في الموقف المشابه للفعل، وبالتالي تجعله قادراً على التنبؤ، ومن أمثلته بحث جوجل، الذي يمكنه التنبؤ عما تبحث عنه[٢].

٢. القدرة على الإدراك والحركة:

من حيث الإدراك، فإن للذكاء الاصطناعي القدرة على استيعاب أساليب متعددة من البيانات كالصوت والصورة ومقاطع الفيديو ومعالجة اللغة الطبيعية، كما يمكن له أن يتعرف على الأنماط والنماذج واستخلاص المعرفة والبيانات بشكل أسرع[٣].

أما بالنسبة للحركة، فقد استطاعت الروبوتات الذكية أن ترتقي في الحركة بشكل مماثل لما يقوم به الإنسان من حركة، بالإضافة إلى تفاعلها مع البيئة المحيطة بها، فتقوم بمجموعة مختلفة من المهام الحركية وبدقة عالية كالمشي والتفاعل مع البشر[٤].

٣. القدرة على التعلم الآلي:

من أهم المزايا والخصائص التي يتمتع بها الذكاء الاصطناعي هو التعزيز الذاتي، والذي يعمل بشكل مستمر، مما يكسبه خبرة وبيانات تراكمية قادرة على تطوير نفسه، ويجعله أكثر كفاءة وفاعلية، بالإضافة إلى خاصية التعليم المستمر الذي يعمل على

(١) عبدالمحسن وآخرون، مرجع سابق، ص٥٢٧.
(٢) خليفة، محمد محمد طه. (٢٠١٨). الذكاء الاصطناعي في ميزان التشريع. مجلة دبي القانونية، ص٣.
(٣) الشهري، مرجع سابق، ص٨٠.
(٤) ساعي، علاء. (٢٠٢٤). الذكاء الاصطناعي. دار رسلان للنشر، الرياض، ص٣٠.

تطوير الخوارزميات والنماذج والأنماط باستمرار، وخاصية التعليم العميق نتيجة استخدام شبكات عصبونية لتحليل البيانات بشكل متقدم، مما يمكنه من اكتساب درجة عالية من الفهم والذكاء[١].

الفرع الثاني

أنواع الذكاء الاصطناعي

يوجد عدة أنواع من تقنية الذكاء الاصطناعي، والتي تتفاوت فيما بينها بقدرتها على التمييز وفهم الأوامر وغيرها من السلوكيات، ويمكن تقسيم الذكاء الاصطناعي إلى ثلاثة أنواع، وهي:

النوع الأول: الذكاء الاصطناعي الضعيف:

وهو أبسط أنواع الذكاء الاصطناعي، حيث يمكنه القيام بوظيفة معينة ويُعطى له ردود أفعال معينة، ولا يمكنه العمل إلا بالظروف البيئية الخاصة به، ومن أمثلة هذا النوع هو الروبوت «ديب بلو» الذي هزم بطل الشطرنج العالمي جاري كاسبروف[٢].

النوع الثاني: الذكاء الاصطناعي القوي:

ويتميز هذا النوع بقدرة كبيرة على جمع وتحليل واكتساب المعارف والبيانات وردود الأفعال، حيث يمتلك خبرة تراكمية لعدد كبير من السلوكيات والأفعال ولديه القدرة على اتخاذ القرارات بذكاء، ومن أمثلة هذا النوع هو برامج المساعدة الذاتية الشخصية، سيارات القيادة، وروبوتات الدردشة الفورية[٣].

النوع الثالث: الذكاء الاصطناعي الفائق:

ويسمى بالذكاء الاصطناعي الخارق وهو لا زال قيد التجارب، وهو أذكى بكثير من أذكى العقول البشرية في كل مجال، ويدخل في الإبداع العلمي والمهارات الاجتماعية والحكمة العامة[٤]، وفي هذا النوع من الذكاء الاصطناعي يمكنه التمييز بين نمطين، النمط الأول:

---

(١) الشهري، مرجع سابق، ص٨٠.

(٢) خليفة، إيهاب. (٢٠١٧). تأثيرات تزايد دور التقنيات الذكية في الحياة اليومية للبشر. مقالة منشورة في الرابط https://futureuae.com/media/20_371c98d6-6b55-4f40-8200-6ffcca032c25.pdf تاريخ الدخول ١٠/١١/٢٠٢٥م.

(٣) الشهري، البراء محمد جمعان، مرجع سابق، ص٧٩.

(٤) قاسم، مرجع سابق، ص٩٦.

يحاول فهم الأفكار البشرية وانفعالاتهم ويملك قدرة محدودة على التفاعل الاجتماعي، أما الثاني: فهي نماذج لنظرية العقل والتعبير لحالتها الداخلية، والتنبؤ بمشاعر الآخرين والتفاعل معها، وتمثل هذه النماذج الجيل الجديد من الآلات فائقة الذكاء[1].

المطلب الثاني

الجرائم الإلكترونية وصورها

تمهيد:

إن التحولات الرقمية السريعة التي شهدها العالم مؤخراً نتيجة التقدم في تكنولوجيا المعلومات والاتصالات والإيجابيات التي قدمتها، جعلت الفضاء السيبراني بيئة حديثة لإنجاز المعاملات وتقديم الخدمات الكترونياً، وصاحب هذا التقدم ظهور سلبيات وجرائم تُرتكب عبر هذا الفضاء الافتراضي وذلك باستخدام أساليب وطرق حديثة ومتنوعة، مما يجعلها بيئة خصبة لارتكاب الجرائم الأكثر تعقيداً وخطورةً، ويُعرف هذا النوع من الجرائم بالجرائم المعلوماتية أو السيبرانية أو الإلكترونية، وتتخذ عدة صور كالنصب والاحتيال والابتزاز والسرقة والتشهير وممكن تصل إلى التجسس على الدول، أو الهجوم على البنى التحتية الرقمية لدول أخرى، لذا سارعت العديد من الدول سن التشريعات وحددت الركائز الأساسية لضمان أمن الفضاء الرقمي من هذه الجرائم، وفي هذا المطلب سنتعرف على هذه الجرائم وصورها.

الفرع الأول

مفهوم الجرائم الإلكترونية وخصائصها

تمهيد:

مع انتشار استخدام الحاسب الآلي والإنترنت، ظهرت جرائم مرتبطة بها تعرف بالجرائم الإلكترونية، وهي جرائم تشكل أكبر تحد أمام رجال القانون والتشريع، لأنها تتطلب قدرات وذكاء في وضع القوانين تقابل الذكاء الذي يتمتع به مرتكبو هذه الجرائم لمعاقبتهم، فالجرائم الإلكترونية تمثل سلوكاً إجرامياً تتم بمساعدة الحاسب الآلي، وفيما يلي سنتعرف على مفهوم هذه الجرائم والخصائص التي تتمتع بها.

---

(١) شادي، عبدالوهاب، الغيظاني، إبراهيم ويحيى سارة. (٢٠١٨). فرص وتهديدات الذكاء الاصطناعي في العشر سنوات القادمة، تقرير المستقبل، ملحق يصدر مع «اتجاهات الأحداث»، ع(٢٧)، ص٢.

تعريف الجريمة لغةً:

الجريمة عند أهل اللغة تأتي بمعنى الجناية وبمعنى الذنب، وقال في لسان العرب لابن منظور: «وجرم إليهم وعليهم جريمة وأجرم: جنى جناية"، والجُرم: التعدي، والجُرم: الذنب، والجمع أجرام وجروم، وهو الجريمة، وقد جرم يجرم جرماً واجترم وأجرم، فهو مجرم وجريم، الجُرم: الذنب والجُرم: مصدر الجارم الذي يجرم نفسه وقومه شراً. وفلان له جريمة إلى أي جُرم والجارم: الجاني والمجرم: المذنب[١].

تعريف المعلوماتية لغةً:

«المعلوماتية» مصطلح مستحدث مشتق من كلمة «معلومات»، والتي تعود للأصل الثلاثي «عَلِمَ»، وهو مَجْموع التِقْنيَّات المُتعلِّقة بالمَعْلُومات ونَقْلِها وخاصَّةً مُعالَجتِها الآليَّة والعَقْليَّة بحَسَب العِلْم الإلكتروني[٢].

تعريف الجريمة الإلكترونية لغة:

يمكن تعريف الجريمة الإلكترونية على أنها «أي مخالفة ترتكب ضد أفراد أو جماعات بدافع جرمي ونية الإساءة لسمعة الضحية أو لجسدها أو عقليتها، سواءً كان ذلك بطريقة مباشرة أو غير مباشرة، وأن يتم ذلك باستخدام وسائل الاتصالات الحديثة مثل الإنترنت، غرف الدردشة، والبريد الإلكتروني[٣].

تعريف الجريمة الإلكترونية اصطلاحاً:

لا يوجد اجماع على تعريف موحد للجريمة الإلكترونية وانما تعددت تعريفاتها، فعرفها ليوكفيلدت وفنسترا وستول «كمصطلح عام لجميع أشكال الجريمة التي تلعب فيها تكنولوجيا المعلومات والاتصالات دورا أساسيا وهنا تقع الكثير من الجرائم ضمن هذا التعريف."[٤]

وتعرف بأنها: الجريمة التي تلعب فيها البيانات الحاسوبية والبرامج الحاسوبية دوراً

(١) لسان العرب – ابن منظور – ج ١٢ – الصفحة ٩١، متوفر في الرابط: https://shamela.ws/book/10226/2 تاريخ الدخول: ٢٠٢٥/١١/١٣م.

(٢) معجم المعاني الجامع، متوفر بالرابط: https://www.almaany.com// تاريخ الدخول: ٢٠٢٥/١١/١٣م.

(٣) ويكبيديا، متوفر على الرابط: https://ar.wikipedia.org/wiki9 تاريخ الدخول: ٢٠٢٥/١١/١٣م.

(٤) مرعي، إسراء جبريل رشاد. (٢٠١٦). الجرائم الإلكترونية: الأهداف – الأسباب – طرق الجريمة ومعالجتها. المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، متوفر على الرابط: https:// democraticac.de/?p=35426 تاريخ الدخول: ٢٠٢٥/١١/١٣م.

رئيسياً في وقع الجريمة المعلوماتية[١].

كما عرفت بأنها: «نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود»[٢].

وقد عرفتها منظمة التعاون الاقتصادي والتنمية بأنها: «كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات و/أو نقلها[٣].

الجريمة الإلكترونية إجرائياً:

من التعاريف السابقة، يمكننا القول بأن الجرائم الإلكترونية هي سلوك أو جناية يستخدم فيها المجني أدوات تقنية المعلومات والاتصالات لإلحاق الضرر بالمجني عليه، سواء ضرر مادي أو نفسي أو أخلاقي.

وتتميز الجرائم الإلكترونية بخصائص فريدة تجعلها تختلف عن الجرائم التقليدية، ومن أهم السمات التي تتميز بها هذه الجرائم هي:

١. جرائم عابرة للحدود:

تتخطى الجرائم الإلكترونية كل الحدود الجغرافية، فنقل البيانات والمعلومات يتم عن طريق جهاز الكمبيوتر وشبكة الإنترنت من دولة إلى أخرى أو عدة دول في نفس الوقت، أي يكون بين الجاني والمجني عليه مئات أو آلالف الكيلومترات[٤].

٢. جرائم سريعة التنفيذ:

لا تتطلب الجرائم الإلكترونية سوى ضغطة زر لتنفيذها، حيث يمكن أن تنقل مئات الملايين من الدولارات من مكان إلى آخر بسرعة متناهية، لكن هذا لا يعني أنها لا تحتاج إلى تجهيز وإعداد قبل تنفيذها[٥].

---

(١) الكعبي، محمد عبيد. (٢٠٠٩). الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت. دار النهضة العربية، القاهرة، ص٣٣.

(٢) القرعان، محمود أحمد. (٢٠١٧). الجرائم الالكترونية. دار وائل للنشر والتوزيع، ص١٩.

(٣) المائل، عبدالسلام، الشربجي، عادل وقابوسة، علي. (٢٠١٩). الجريمة الالكترونية في الفضاء الالكتروني. مجلة آفاق للدراسات السياسية والدولية، المركز الجامعي ايليزي ISNN ٢٦٠٢-٦٥٤٦، ص٢٤٦. (٢٤٢-٢٥٥).

(٤) بوحفص، راوية وبوستة، إيمان. (٢٠١٨). الجريمة الالكترونية في التشريع الجزائري. رسالة ماجستير منشورة، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، ص١١. (١-٧٠).

(٥) المائل وآخرون، مرجع سابق، ص ٢٥١.

٣. جرائم تنفذ عن بعد:

لا تتطلب الجرائم المعلوماتية وجود المجرم في مسرح الجريمة، فيمكن أن يكون الفاعل في دولة أخرى بعيدة كل البعد عن الدولة الموجود فيها الضحية، فيرتكب جريمته من خلال الولوج إلى الشبكة المعلوماتية[١].

٤. جرائم ناعمة ومغرية:

تتميز الجرائم المعلوماتية بأنها جرائم ناعمة لا تحتاج لأدنى مجهود عضلي، فقط تحتاج إلى مهارة وذكاء من المجرم المعلوماتي ودراية كافية بالأدوات التقنية التي تستخدم لارتكابها[٢].

٥. جرائم يصعب اكتشافها وإثباتها:

لا تحتاج الجرائم الإلكترونية إلى أي عنف أو اقتحام أو سفك دماء، وإنما هي بيانات يمكن نقلها أو تعديلها أو محوها، لذا من الصعب اكتشافها ومن ثم معاقبة مرتكبيها، كما أنها تتميز بصعوبة إثباتها لأنها لا تترك أي أثر خارجي ومرئي لها، لأن هذه الجرائم تستخدم نبضات إلكترونية في نقل المعلومات لذا من الصعب إثباتها[٣].

٦. جرائم فادحة الاضرار:

أكدت الشركة العالمية المتخصصة في أمن المعلومات «انتل سكيورتي» بأن الخسائر التي تكبدتها الشركات والمؤسسات الحكومية ضخمة نتيجة الجرائم الإلكترونية، بالأخص المجال الاقتصادي والمؤسسات المالية والبنوك[٤].

٦. قلة الإبلاغ عن وقوع الجرائم الإلكترونية:

لا يتم الإبلاغ عن وقوع هذه الجرائم إما لعدم معرفة الضحية بالجريمة التي ارتكبت

---

(١) مركز هاردو لدعم التعبير الرقمي. (٢٠١٤). الجريمة الالكترونية وحجية الدليل الرقمي في الإثبات الجنائي. القاهرة، ص ١٦. (١-٤٠).

(٢) الصحفي، روان بنت عطية الله. (٢٠٢٠). الجرائم السيبرانية. المجلة الإلكترونية الشاملة متعددة التخصصات ع(٢٤)، ص١٣. (١-٥٣).

(٣) عبداللطيف، عبدالرؤوف وخذيري، عفاف. (٢٠٢٢). مكافحة الجريمة الالكترونية في التشريع الجزائري. رسالة ماجستير منشورة من كلية الحقوق والعلوم السياسية، جامعة الشيخ العربي التبسي، الجزائر، ص ١٣. (١-١٠١).

(٤) عاقلي، فضيلة. (٢٠١٧). الجريمة الالكترونية وإجراءات مواجهتها في التشريع الجزائري. المؤتمر الدولي الرابع عشر حول الجريمة الالكترونية، طرابلس، ص٨.

بحقها، أو خوفاً من التشهير، لذا فإن معظم هذه الجرائم اكتشفت بالصدفة بعد وقت طويل من وقوعها[١].

الفرع الثاني

صور الجرائم الإلكترونية ودوافع ارتكابها

توجد أربع صور رئيسية للجرائم الإلكترونية، وكل صورة أو نوع يندرج تحته قائمة من الجرائم، وهي:

١. الجرائم الإلكترونية الواقعة على الأشخاص[٢]:

إن جميع الأديان والتشريعات حمت الحياة الخاصة للأفراد، فلكل شخص منا حياته وأسراره الشخصية التي لا يجوز لأي أحد انتهاكها والاطلاع عليها بغير إذن، والجريمة الإلكترونية تكمن في انتهاك حرمة الأشخاص عبر الدخول إلى أجهزتها والاطلاع على بياناتها الشخصية وصورها وكل المعلومات التي تتعلق بتلك الأشخاص، وهي جريمة قائمة بحد ذاتها يعاقب عليها القانون، ويكون الاعتداء على الأشخاص من خلال:

- الاختراق وإتلاف المعلومات الموجودة في أجهزة تلك الأشخاص.
- السب والقذف الإلكتروني.
- التشهير الإلكتروني ونشر معلومات تشوه سمعة ومكانة تلك الأشخاص.
- الابتزاز الإلكتروني.
- التهديد الإلكتروني.
- النصب والاحتيال الإلكتروني.
- الاستغلال الجنسي للأطفال إلكترونياً، وهم أكثر فئة معرضة للاستغلال الجنسي عبر نشر صورهم وفيديوهات مخلة بهم.
- التنصت والتجسس الإلكتروني.

٢. الجرائم الإلكترونية على الأموال[٣]:

---

(١) عبداللطيف واخرون، مرجع سابق، ص١٨.

(٢) الحلبي، خالد عيادي. (٢٠١١). إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت. دار الثقافة، عمان، ص٦١.

(٣) راوية وآخرون، مرجع سابق، ص١٥.

إن تزايد المعاملات الإلكترونية من بيع وشراء على مواقع الإنترنت، أظهر جريمة السرقة إلكترونية، وهي السطو على النقود بطريقة غير مشروعة عن طريق التحويل الإلكتروني والقرصنة على حسابات البنوك واختلاس بيانات العملاء وتحويل الأموال من حسابات العملاء إلى حسابات المجرمين باستخدام الحاسب الآلي والإنترنت، كما توجد عدة صور من الجرائم الإلكترونية الواقعة على الأموال، كالآتي:

- تجارة المخدرات عبر الإنترنت.
- الاتجار بالبشر.
- قرصنة البرمجيات.
- جريمة القمار عبر الإنترنت.
- جريمة غسل الأموال.

٣. الجرائم الإلكترونية على الملكية الفكرية:

وتتضمن هذه الجرائم الاعتداء على العلامات التجارية وبراءة الاختراع، وأيضاً نسخ البرامج وإعادة تصنيعها كل هذا يمثل جريمة على الحقوق المالية والأدبية[١].

٤. الجرائم الإلكترونية على أمن الدولة:

تتضمن هذه الجرائم إنشاء مواقع لمنظمات إرهابية، والترويج لأفكارها والتواصل مع أعضائها، وتمويلها لاختراق أجهزة الدولة والحصول على بيانات تمس الأمن الوطني للبلد[٢].

وهناك عدة دوافع لارتكاب الجرائم الإلكترونية، وهي:

١. تحقيق الربح المادي:

إن من أهم الدوافع لارتكاب الجرائم الإلكترونية هو الطمع والاستيلاء على المال، وقد أثبتت الدراسات أن القطاعات المالية والمصرفية من أكثر القطاعات عرضة للجرائم الإلكترونية، حيث تبلغ نسبة ٤٣٪ من إجمالي الجرائم الإلكترونية دافعها الربح المادي[٣].

٢. إثبات التفوق العلمي:

(١) الشمري، غانم مرتضى. (٢٠١٦). الجرائم الإلكترونية. الدار العلمية الدولية، عمان، ص٥٣.
(٢) الصحفي، مرجع سابق، ص٢٠.
(٣) وزارة العدل الكويتية. (٢٠١٨). الجرائم الإلكترونية. معهد الكويت للدراسات القضائية والقانونية، الكويت، ص١٧.

يوجد لبعض مجرمي الجرائم الإلكترونية رغبة في قهر الحاسب الآلي وإثبات قدرتهم على اختراقه ودخوله غير المشروع لأنظمته، لذا نجد أن معظم مجرمي هذه الجرائم صبية وصغار بالسن تريد أن تدخل المنافسة في عالم المعلوماتية[١].

٣. الرغبة في الانتقام:

يعتبر دافع الانتقام من دوافع ارتكاب الجريمة الإلكترونية، فغالباً تصدر هذه الجرائم من شخص يملك معلومات كبيرة عن شخص أو مؤسسة معينة أو شركة يحس تجاهها بالرغبة بالانتقام نتيجة فصله تعسفياً أو حرمانه من حوافز ومكافآت، فيقدم على هذه الجريمة إشفاءً لما بداخله من قهر تجاه هذه الشخص أو المؤسسة[٢].

٤. الشعور بالنقص:

يدفع الشعور بالنقص وهو خلل في الناحية النفسية مرتكبي الجريمة الإلكترونية إلى تعويض النقص والعجز الذي يشعرون به، فيقدمون على تنفيذ هذه الجرائم إرضاءً لشعورهم بالنقص[٣].

٥. حرية التعبير وتداول المعلومات:

قد تدفع حرية التعبير في كثير من الدول إلى نشر المعلومات السرية للأفراد والشركات الكبرى، والتي تعتبر معلوماتها سرية، مما يدفع الكثير من مرتكبي هذه الجرائم إلى اختراق بيانات ومعلومات بغرض نشرها وإشاعتها لا بغرض الربح المادي[٤].

(١) الشناوي، محمد. (٢٠٠٧). جرائم الإنترنت وبطائق الائتمان والجريمة المنظمة. دار الكتب الحديث، ص٤٦.
(٢) وزارة العدل الكويتية، مرجع سابق، ص١٨.
(٣) وزارة العدل الكويتية، مرجع سابق، ص١٩.
(٤) وزارة العدل الكويتية، مرجع سابق، ص٢٠.

المطلب الثالث

مجالات وتطبيقات الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية

تمهيد:

يعد الذكاء الاصطناعي من الأدوات التقنية الحديثة التي شاع استخدامها مؤخراً في أغلب العلوم والتخصصات بما في ذلك علم مكافحة الجرائم، والذي يقوم بتحليل البيانات التراكمية وإعطاء نتائج استباقية للحد من الجريمة بما فيها الجريمة الإلكترونية موضوع بحثنا، وفي هذا المطلب سنتعرف على أهم مجالات وتطبيقات الذكاء الاصطناعي لمواجهة الجرائم الإلكترونية.

الفرع الأول

مجالات استخدام الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية

يمثل الذكاء الاصطناعي سلاحاً فتاكاً في مكافحة الجريمة ويدخل في العديد من المجالات الخاصة بها، وفيما يلي سنتعرف على أهم المجالات التي يستخدم فيها الذكاء الاصطناعي في مواجهة الجرائم الإلكترونية:

١. الإرهاب السيبراني:

تعد جرائم الإرهاب السيبراني من أكثر الجرائم التي ظهرت في الآونة الأخيرة نتيجة انتشار البرامج الخبيثة لأجهزة الحاسوب والموبايل، حيث يستطيع مجرموها ويعرفون بـ «الإرهابيين» تنفيذ أخطر أنواع الجرائم السيبرانية أو الإلكترونية كربط عدة قنابل إلكترونية مؤقتة في عدة دول بشبكة موحدة وتفجيرها عن بعد في دولة معينة، تغيير تركيبات الأدوية من خلال اختراق مصانع الأدوية وبالتالي قتل العديد من الأبرياء، كما يمكن لمجرميها أن يقوموا بتعطيل الشركات التجارية العالمية مثل شركات الطيران والبورصات وتغيير مستويات احتياطي البنوك، كما يمكن للإرهابيين أن يغيروا مستويات الغاز الطبيعي ويتسببوا في تدمير صمام الأمان، أو اختراق الشبكة الكهربائية وتعطيل عدادات الكهرباء[1].

(١) إبراهيم، علي أحمد. (-). تطبيقات الذكاء الاصطناعي في مواجهة الجرائم الإلكترونية. المجلة القانونية، ص٢٨٢٠. (٧٥٨-٢٥٣٧).

ويظهر دور الذكاء الاصطناعي في مكافحة الإرهاب السيبراني عبر شبكات التتبع بالتصوير بالأقمار الصناعية، وتحديد الموقع الجغرافي للمجرمين من خلال البيانات المستمدة من هواتفهم المحمولة، واستخدام كاميرات شبكية لضبط مراقبة البث المباشر للأنشطة غير القانونية، حيث تستطيع هذه الكاميرات التعرف على الوجه ومقارنتها بأوجه المجرمين المدرجين في القائمة السوداء المخزنة لدى الأجهزة الأمنية، كما يستخدم الذكاء الاصطناعي في حماية رجال الأمن وذلك بعدم الاتصال المباشر مع مجرمي الإرهاب السيبراني[1].

٢. السوق السوداء للمعلومات[2]:

إن انتشار أسواق المعلومات فتحت المجال إلى استهدافها من قبل مجرمي الإنترنت، فالإعلانات الموجودة في الإنترنت تحتوي على قاعدة بيانات لأفراد وشركات ومؤسسات، وهذه المعلومات هامة للغاية ويمكن أن تتعرض للسرقة، وتسمى هذه العملية «السوق السوداء للمعلومات»، والتي تمثل السجلات الطبية، البريد الإلكتروني، ومن أمثلة ذلك:

- الحصول على الرقم السري: قامت مجموعة من المجرمين بوضع كاميرا ذكية لتلتقط الأرقام السرية التي يتم إدخالها وتسجلها وتبحث عنها في إيصالات البنوك.
- سرقة رقم بطاقة الائتمان: من السهل سرقة رقم بطائق الائتمان والتي تستخدم في البيع والشراء عبر الإنترنت، أو الدخول إلى المتاجر والمواقع التي يتم الشراء منها وسرقة هذه الأرقام.
- أجهزة الصراف الآلي الخادعة: قامت مجموعة من المجرمين بوضع صراف آلي مزيف أو خادع في أحد المراكز بالولايات المتحدة، ويعمل كالجهاز الحقيقي، يدخل المستخدم بياناته وكلمة السر ويتم تسجيلها ومن ثم يخبره بأن الصراف الآلي تعطل، ومن ثم يقومون باستخدام البيانات وإدخالها في صرافات حقيقية وسحب مبالغ نقدية منها.
- قواعد بيانات المعلومات: عند الشراء عبر الإنترنت، فإن مواقع المتاجر تقوم باحتفاظ بيانات بطاقات الائتمان للمتعاملين حتى يسهل الشراء مرة أخرى،

(١) قاسم، مرجع سابق، ص١٠٤.
(٢) إبراهيم، علي أحمد، مرجع سابق، ص٢٨٢٢.

بحيث لا يدخل العميل البيانات في كل عملية شراء، وبالتالي يصبح من السهل على مجرمي المعلومات سحب البيانات واستخدامها في سرقة أموال العملاء.

٣. الابتزاز السيبراني:

إن التطور الحاصل في التقنيات الحيوية (البارومتري) والتي تقتصر على عدد قليل من أجهزة المستخدمين، وبمجرد أن تصبح وسيلة مصادقة لدخول الحسابات على الإنترنت، فإنها تصبح معرضة للسرقة، مما يسهل على الجناة ابتزاز المستخدمين وطلب فدية مقابل عدم تدمير حساباتهم، وقد بدأت هذه الهجمات الإلكترونية وعملية ابتزاز المستخدمين ولكن على نطاق ضيق، ومن المحتمل في المستقبل أن ترتفع نسبة الهجمات وتطال المنازل والسيارات وهجمات الاصطياد ودفع الفدية لجعلها تتوقف[١].

الفرع الثاني

تطبيقات الذكاء الاصطناعي المستخدمة في مكافحة الجريمة الإلكترونية

يساعد ويساهم الذكاء الاصطناعي في كثير من الأعمال الخاصة بالمجال الأمني، ومواجهة الجريمة ومن ضمنها الجريمة الإلكترونية، من خلال عدد من تطبيقاته التي تقوم على تصنيف المجرمين والتنبؤ بأعمالهم، ووضع استراتيجيات تسهم في تحقيق العدالة، وفيما يلي سنتعرف على تطبيقات الذكاء الاصطناعي المستخدمة في مكافحة الجريمة الإلكترونية في المجال الأمني والقانوني:

١. تطبيقات الذكاء الاصطناعي في النظام القانوني والقضائي:

تسهم تطبيقات الذكاء الاصطناعي في المجال القانوني والقضائي في العديد من المهام الذي يقوم بها، كتوفير قاعدة بيانات عن القضايا والمشاكل القانونية المتشابهة، كما يقوم بمراجعة المستندات القانونية ويضع عليها علامة باعتبارها ذات صلة بقضية معينة، ويقلل الوقت اللازم لمراجعتها والرجوع إليها وقت الحاجة، وبالتالي يُمكن القضاة والقانونيين من استخراج الأدلة والبيانات بوقت قياسي مما يجعلهم يتفرغون للمواضيع الأكثر تعقيداً لتطبيق القانون، وكذا يقوم بمراجعة صياغة العقود باستخدام برامج ومنصات إلكترونية ومطابقتها بالضوابط والمعايير لعقود الشركات الكبرى وإيضاح الخلل أو الانحراف فيها، ويساهم في توقعات المستقبل من خلال التعرف على

(١) إبراهيم، علي أحمد، مرجع سابق، ص ٢٨٢٣.

المستجدات القانونية المستقبلية عبر آلية الترميز التنبؤي[١].

ومن تطبيقات الذكاء الاصطناعي في المجال القانوني هو استخدام الروبوتات القانونية، حيث يلعب الروبوت دور القاضي، حيث يجد المتقاضون أنفسهم أمام قاض يقرأ أوراق الدعوى ويحقق فيها ويصدر حكمه في القضية، أيضاً تتجلى مظاهر الذكاء الاصطناعي في زيادة كفاءة المحامين أمام القضاء، من خلال استخدام الأساليب الإلكترونية الحديثة في المجال القانوني[٢].

٢. الشرطة التنبؤية:

تستخدم أجهزة الأمن تقنيات وتطبيقات الذكاء الاصطناعي للتنبؤ عن الجريمة، فتستخدم معدات وأجهزة تحليلية متطورة، حيث تستخدم هذه التقنية الذكية في تحليل البيانات الضخمة المتعلقة بالمجرمين والمشتبه بهم، والتنبؤ بأماكن والتوقيت الزمني لارتكاب الجريمة، بحيث يتم تكثيف الحماية والدوريات في تلك المواقع، محاولة منها إيقاف الجريمة قبل وقوعها، وبالتالي يعزز قدرة الأجهزة الأمنية على أداء مهامها بكل كفاءة وفاعلية ويحمي المجتمعات من الجرائم المتوقعة[٣]، وتعرف الشرطة التنبؤية بأنها «الشرطة التي تقودها المعلومات المستخلصة من الاستخبارات»، فهي تحول مفهوم الشرطة التقليدي إلى مفهوم جديد مرتبط بالتكنولوجيا يرصد الجريمة والتنبؤ بها قبل وقوعها، مما يعزز فاعليتها في مواجهة الجرائم[٤].

٣. التحقيق الرقمي:

تساهم تقنية الذكاء الاصطناعي في زيادة خبرة ومهارات رجال التحقيق الجنائي، حيث يستخدم الذكاء الاصطناعي في تحليل الأنشطة الجنائية السابقة وتوقع الأنشطة الجنائية المحتملة، ومن هذه التطبيقات:

أ. تطبيقات الذكاء الاصطناعي في تحليل البيانات:

إن من أهم تطبيقات الذكاء الاصطناعي هو تحليل البيانات والتي تعلب دوراً مهماً في

(١) إبراهيم، خالد ممدوح. (٢٠٢٢). التنظيم القانوني للذكاء الاصطناعي. دار الفكر القانوني، الإسكندرية، مصر، ص٤٠.
(٢) عبدالنور، عبدالحق وحماس، عمر. (٢٠٢٤). الذكاء الاصطناعي بين ارتكاب الجرائم المالية والوقاية منها. مجلة العلوم القانونية والاجتماعية، ٩(٣)، ص٤٩٦. (٤٨٨-٥٠٨).
(٣) غازي، مهند سعد. (٢٠٢٤). دور الذكاء الاصطناعي في تطوير عمل المنظومة الأمنية. جامعة المنصورة، كلية الحقوق، قسم القانون الجنائي، مصر، ص٦.
(٤) غازي، مرجع سابق، ص٨.

التخطيط والتنفيذ والقضاء على الجريمة والكشف عنها قبل وقوعها، فيستخدم تطبيق الذكاء الاصطناعي في تحليل البيانات الضخمة بكافة أنواعها، واشتقاق واستنباط الأدلة منها[١].

ب. تطبيقات الذكاء الاصطناعي في تحليل الصور والفيديوهات:

تستخدم هذه التطبيقات من الذكاء الاصطناعي كاميرات مراقبة ذكية، لديها القدرة على تحليل الصور والفيديوهات لتحديد أماكن تواجد المشتبهين بالجريمة[٢].

ج. تطبيقات الذكاء الاصطناعي في المراقبة:

والمقصود بالمراقبة هو الملاحظة السرية للأشخاص المشتبه بهم، والأماكن المتوقع وجودهم فيها، وذلك عن طريق أجهزة الذكاء الاصطناعي للتصوير الضوئي والتلفزيوني، والمعاينة الفورية لمسرح الجريمة دون علم مرتكبيها، فتعطي صورة مباشرة وحية للجريمة، لذا تستخدم الرادارات والعدسات الضوئية في الأماكن العامة والأسواق وكذا البنوك والمطارات والأماكن الهامة[٣].

د. تطبيقات الذكاء الاصطناعي في تحليل بيانات شبكات التواصل الاجتماعي:

تستخدم شبكات التواصل الاجتماعي العديد من تطبيقات الذكاء الاصطناعي، لمواجهة السلبيات التي تظهر في هذه المواقع، كالمحتوى المتطرف، أو الانتحار، أو الدعارة والفجور وغيرها[٤].

٤. أدلة الإثبات الجنائية:

الإثبات الجنائي يقصد به إقامة الدليل الذي يستند إليه القضاء في حكمه، ومع تطور العلم والتكنولوجيا ظهرت أدلة مختلفة بطبيعتها عن الأدلة التقليدية التي تتسم بالعنف والتعذيب، أدلة قائمة على أساس علمي متطور تعرف بالأدلة الإلكترونية أو الرقمية، ويهدف علم الذكاء الاصطناعي إلى فهم طبيعة الذكاء الإنساني، حيث يدعم تطبيق القانون عن طريق الآلات والأجهزة التي تقوم بفحص الأدلة الإلكترونية ومراجعتها ودورها في إثبات الوقائع والجرائم لتطبيق الأحكام القانونية[٥].

(١) الشهري، مرجع سابق، ص٨٣.
(٢) الشاعر، مرجع سابق، ص ٢٦.
(٣) الشهري، مرجع سابق، ص٨٣.
(٤) البشري، محمد الأمين. (٢٠١١). الأساليب الحديثة للتعامل مع الجرائم المستحدثة من طرف أجهزة العدالة الجنائية. جامعة نائف العربية للعلوم الأمنية. الرياض، ص٦.
(٥) العباسي، ميسون بشير والجرجري، فارس علي. (٢٠٢٥). الذكاء الاصطناعي وحجيته في الإثبات المدني: دراسة مقارنة. مجلة كلية القانون للعلوم القانونية والسياسية، ١٤(٥٣)، ص٦٢١. (٦٠٨-٦٣٤).

المطلب الرابع

تحديات مواجهة الجرائم الإلكترونية بواسطة الذكاء الاصطناعي

تمهيد:

في ظل التطور الرقمي وانتشار الإنترنت، برز نوع خاص من الجرائم التي تهدد المجتمع اليمني، وهي الجرائم الإلكترونية، وصاحب هذا التطور مؤخراً توظيف الذكاء الاصطناعي الذي يعتبر ثورة تكنولوجية قادرة على إحداث تغيير إيجابي في شتى مجالات الحياة، وعلى وجه الخصوص مجال مكافحة الجريمة الإلكترونية موضوع بحثنا، إلا أن هذه الثورة تنصدم بعدد من المعيقات والتحديات التي تحول دون توظيفها في بلادنا نتيجة لكثير من الاعتبارات الأخلاقية والموثوقية والأمنية والمالية والبشرية والقانونية والبنى التحتية التي تدعم عمل تطبيقات الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية في اليمن، وفي هذا المطلب سنعرض أهم هذه التحديات.

١. ضعف البنية التحتية:

إن من أهم متطلبات توظيف الذكاء الاصطناعي هي البنية التحتية القوية، والمعروفة أيضًا باسم مجموعة الذكاء الاصطناعي، وهي مصطلح يشير إلى الأجهزة والبرامج اللازمة لإنشاء ونشر التطبيقات والحلول المدعومة بالذكاء الاصطناعي، والسبب الرئيس إلى أن تطبيقات الذكاء الاصطناعي تحتاج بنية تحتية قوية هو الكمية الهائلة من الطاقة اللازمة لتشغيل أعباء الذكاء الاصطناعي، حيث تعتمد البنية التحتية على زمن انتقال قصير في البيئات السحابية، ومعالجة للرسومات أقوى من المعالج الذي تحتاجه البيئة التقليدية[١].

إن تطوير حلول الذكاء الاصطناعي يتطلب موارد حوسبية ضخمة وبنية للبيانات متينة وقوية، إذ يعتمد نجاح تطبيق الذكاء الاصطناعي على توفر واستخدام بيانات ضخمة وعالية الجودة، تكون قادرة على التكامل مع مصادر بيانات متدفقة من أدوات مختلفة، وهذا بحد ذاته يشكل تحدياً لبعض الأنظمة، نظراً لضعف بنيتها الأساسية أو لمحدودية توافر بياناتها، كما هو الحال في الأنظمة العربية[٢].

---

(١) الموقع الرسمي لشركة IBM عبر الرابط: https://www.ibm.com/sa-ar/think/topics/ai-infrastructure تاريخ الدخول: ٢٢/١١/٢٠٢٥م.

(٢) الهيئة السعودية للبيانات والذكاء الاصطناعي. (٢٠٢٥). الذكاء الاصطناعي التوكلي، تقنياته وتطبيقاته الوطنية. ص٥٩

وبالنظر إلى هذه البنية التحتية ومقارنتها بما تحتاجه اليمن من بنية تحتية قادرة على تطبيق أنظمة الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية، نجد أنه وفي الوقت الراهن وما تمر به اليمن من حروب وأزمات، خلقت صعوبة مطلقة ونتيجة هشاشة البنى التحتية والتي تحتاج طاقة كبيرة لتشغيلها، ناهيك عن الميزانية الكبيرة اللازمة لشراء معدات وأجهزة وبرامج قادرة على تشغيل تطبيقات الذكاء الاصطناعي.

٢. نقص الكفاءات البشرية المتخصصة:

تعد القدرات البشرية أحد أهم أبعاد الذكاء الاصطناعي، إذ يعتمد نجاحه على الكفاءات التي تعمل على تصميم النماذج وتطوير الخوارزميات، وتواجه المؤسسات نقصاً حاداً في الكوادر المتخصصة في مجال الذكاء الاصطناعي، إذ يتطلب تشغيله وتطويره وإدارته مهارات متقدمة، وقد أكدت شركة ديلويت بأن نقص الكوادر المتخصصة بالذكاء الاصطناعي تعد من أكبر المعيقات[١]، لأنها تتطلب للتعامل مع تعقيدات الذكاء الاصطناعي ونشره وجود فريق متخصص يقوم بمجموعة من الأدوار المطلوبة، كعالم بيانات يركز على أنماط البيانات والخوارزميات والنماذج المطلوبة، مهندس للتعلم الآلي، مطور برمجيات، ناهيك عن الكفاءات البشرية لتأدية أدوار الرقابة عالية القيمة، وقد أشارت إحدى دراسات منظمة التعاون الاقتصادي والتنمية (OECD) إلى أن تطوير المهارات التقنية المرتبطة بالذكاء الاصطناعي كعلم البيانات والأمن السيبراني وتعلم الآلة والمهارات التحليلية والإبداعية والفكرية، يعد شرطاً أساسياً لتطبيق أنظمة الذكاء الاصطناعي، كما أشارت منظمة اليونسكو (UNISCO) إلى أن دمج المهارات الأخلاقية ومهارات متعددة التخصصات ضمن إعداد الكفاءات البشرية في مجال الذكاء الاصطناعي[٢]، وبالنسبة لتوفر الكفاءات البشرية المتخصصة بتقنيات الذكاء الاصطناعي لمكافحة الجريمة في اليمن، يكمن من خلال استخدام تطبيقات الكاميرات الذكية التي لديها القدرة على تحليل الصور لاكتشاف أماكن المشبوهين أو المطلوبين، وكذا استخدام طائرات المراقبة الجوية الذكية (الدرون) لتتبع المجرمين والمشبوهين بارتكاب الجرائم سواء التقليدية أو الإلكترونية.

٣. قصور النصوص التشريعية:

إن العلاقة بين القانون والذكاء الاصطناعي تكمن في وجود إطار أو مسوغ

(١) Deloitte. Insghts. Development Under: agents AI generative A: Deloitte. Insghts (٢٠٢٤).

(٢) الهيئة السعودية للبيانات والذكاء الاصطناعي. (٢٠٢٥). الذكاء الاصطناعي التوكلي، تقنياته وتطبيقاته الوطنية. ص٣٠.

قانوني ينظم استخدام وتطبيق تقنيات الذكاء الاصطناعي؛ ليحمي حقوق الأفراد من خلال توفير آليات للمساءلة والتعاون في هذا المجال، وفيما يخص التشريع اليمني فإنه لا يزال قاصراً عن دخول التقنيات الحديثة في مكافحة أو مساءلة مرتكبي الجرائم الإلكترونية، والتي انتشرت بشكل كبير مؤخراً في المجتمع اليمني، واكتفى بالطرق التقليدية في إجراءات التحري والتحقيق والمحاكمة في الجرائم الإلكترونية[1].

إن خطورة الجرائم الإلكترونية قد تخطت في أساليبها وتقنياتها الجرائم التقليدية، فتطاولت على المعلومات والأموال والاحتيال والتجسس وتدمير البنى التحتية لدولة معينة من خارج حدودها، وتهديد الأمن القومي للبلد، وخصوصية اليمن في الآونة الأخيرة يجعلها هدفاً للإرهاب والتجسس الخارجي، نظراً للحروب والصراعات التي تعاني منها بلادنا منذ أكثر من عقد، وبالتالي القصور الموجود في النصوص القانونية وعدم إقرار مشروع قانون جرائم تقنية المعلومات يمثل عقبة كبرى أمام تنفيذ العقوبات المستحقة لمرتكبي الجرائم الإلكترونية.

٤. شحة الموارد المالية:

ويقصد بالموارد المالية قدرة المنشأة المالية وميزانيتها المحددة على الإنفاق على دعم الابتكارات وتنفيذ أنظمة الذكاء الاصطناعي، حيث يتطلب البحث والتطوير والبنية التحتية الخاصة بالذكاء الاصطناعي وتصميمه واختباره مبالغ مالية هائلة[2]، لذا فإن تبني تقنية الذكاء الاصطناعي ليس بالشيء السهل، وبالذات على بلد كاليمن محدود الموازنة العامة للدولة منذ أكثر من عقد نتيجة الحصار وعدم تصدير النفط والغاز والذي يمثل حوالي ٨٠٪ من الإيراد العام، بالإضافة إلى الانقسامات والوضع اليمني الذي تمر به بلادنا، وعدم صرف ورواتب موظفي الدولة بانتظام، وبالتالي من الصعب تبني هذه التقنية سواء في مكافحة الجرائم أو في المجالات الأخرى.

٥. تحديات الخصوصية:

تعتمد تقنيات الذكاء الاصطناعي على قواعد البيانات التي تمثل المحرك الأساسي لتشغيل الذكاء الاصطناعي، ومن بين البيانات المعتمدة عليها هي البيانات الشخصية،

(١) قاسم، مرجع سابق، ص١٠٩.

(٢) الهيئة السعودية للبيانات والذكاء الاصطناعي. (٢٠٢٤). تبني أنظمة الذكاء الاصطناعي. الطبعة الثانية، ص٨.

إذ تُعد مورداً أساسياً في عصرنا الرقمي، حيث تعتبر خصوصية البيانات حقاً لكل شخص طبيعي كفله الدستور والقانون، لذا تحرص المجتمعات على كفالة هذا الحق وتعتبره حقاً مستقلاً بذاته، وقد أكدت الشريعة الإسلامية على حماية هذا الحق، كما جاء في قوله تعالى: ﴿يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَدْخُلُوا بُيُوتًا غَيْرَ بُيُوتِكُمْ حَتَّى تَسْتَأْنِسُوا وَتُسَلِّمُوا عَلَى أَهْلِهَا ذَلِكُمْ خَيْرٌ لَكُمْ لَعَلَّكُمْ تَذَكَّرُونَ، فَإِن لَّمْ تَجِدُوا فِيهَا أَحَدًا فَلَا تَدْخُلُوهَا حَتَّىٰ يُؤْذَنَ لَكُمْ وَإِن قِيلَ لَكُمُ ارْجِعُوا فَارْجِعُوا هُوَ أَزْكَىٰ لَكُمْ وَاللَّهُ بِمَا تَعْمَلُونَ عَلِيمٌ﴾[1]، لذا حظي هذا الحق باهتمام كبير من قبل المنظمات الدولية والدساتير والنظم القضائية[2].

كما أنه في ظل التطور المتسارع في الأجهزة التقنية والذكية ومواقع التواصل الاجتماعي في عصرنا الحالي، برز مصطلح الخصوصية على نطاق واسع، حيث اعتبرت الخصوصية بمثابة البيانات الشخصية، أي حق يجب أن يحترم وفق القانون، ومؤخراً ظهور تطبيقات الذكاء الاصطناعي الذي يحاكي الذكاء البشري، والتي تعتمد على جمع بيانات شخصية هائلة تستخدم لأغراض معينة مثل تخصيص الخدمات والإعلان والبحث وغيرها، وبالتالي فإن خصوصية الأفراد والمؤسسات تتعرض إلى تحديات فيما يتعلق بحمايتها وأمن بياناتها[3].

وفيما يخص حماية البيانات الشخصية للمواطن اليمني، فقد كفلته كافة القوانين وأهمها قانون رقم (١٣) لسنة ٢٠١٢ بشأن حق الحصول على المعلومات، والذي نصت فيه المادة (٢٥) الفقرة (أ-ب): على الموظف المختص رفض أي طلب حصول على المعلومات إذا كانت هذه المعلومات تحتوي على[4]:

أ - المعلومات التي من المتوقّع في حال الإفصاح عنها، تعريض حياة فرد ما أو سلامته الجسدية للخطر.

ب- البيانات الشخصية، التي من شأن الإفصاح عنها أن يشكل انتهاكاً غير منطقي لخصوصيات الفرد، ما لم تكن البيانات الشخصية متصلة بواجب أو وظيفة أو منصب عام يشغله هذا الفرد.

وبالنظر إلى تقنية الذكاء الاصطناعي الذي يعتمد بشكل أساسي على البيانات مع

(١) سورة النور اية ٢٦-٢٧.

(٢) الإدريسي، عبدالسلام. (٢٠٢٤). حماية الخصوصية أمام تحديات الذكاء الاصطناعي. مجلة الذكاء الاصطناعي والتنمية الإقليمية المستدامة، المغرب، ص٢. (١-٢١).

(٣) ضيف الله، زينب. (٢٠٢٣). الذكاء الاصطناعي والقانون. مجلة القانون والعلوم البيئية، مج(٢)، ع(٣).

(٤) قانون (١٣) لسنة ٢٠١٢ بشأن حق الحصول على المعلومات.

عدم وجود قانون في اليمن يحمي البيانات الشخصية على مواقع التواصل الاجتماعي أو التطبيقات الذكية، مما يجعلها متاحة للانتهاك، وبالتالي عرضة للجرائم الإلكترونية كالنصب والسرقة.

٦. التحديات الأخلاقية:

تمثل الأبعاد الأخلاقية المرتبطة بالذكاء الاصطناعي تحدياً خصوصاً فيما يتعلق بالعدالة والمساءلة والشفافية والأمن المجتمعي، حيث تعكس أنظمة الذكاء الاصطناعي ما تدربت عليه، مما يؤدي أحياناً إلى اتخاذ قرارات غير صائبة، وفيما يلي تبيان المخاطر والتحديات المتعلقة بالبعد الأخلاقي للذكاء الاصطناعي[١]:

- التحيز والتمييز في القرارات الذكية:

أظهرت بعض أنظمة الذكاء الاصطناعي تمييزاً في القروض والتوظيف، حيث تنحاز وتفضل فئات عن فئات أخرى، أيضاً تصميم تقنيات التعرف على الوجه قد تكون أقل دقة لبعض الفئات العرقية.

- المساءلة والشفافية:

التحدي الأخلاقي الأكبر هو تحديد المسؤولية عن وقوع أخطاء في قرارات الذكاء الاصطناعي المؤثرة في حياة البشر.

- استخدام الذكاء الاصطناعي في الأماكن الحساسة:

يستخدم الذكاء الاصطناعي في مجالات حساسة كالطب والقانون ويحمل وعوداً باهرة، إلا أنه محفوف بالمخاطر، إذ يؤدي خطأ طبي أو قانوني دون إشراف بشري إلى كارثة.

- انتشار المعلومات المضللة:

قد يؤدي استخدام تقنيات الذكاء الاصطناعي في توليد النصوص والصور والفيديوهات المزيفة إلى أزمة ثقة بالمعلومات الرقمية وتهدد الأمن المجتمعي.

من الملاحظ أن التحديات الأخلاقية مرتبطة بالإطار التنظيمي والتشريعي لاستخدام تقنية الذكاء الاصطناعي، وكما هو معلوم مسبقاً، أن اليمن لم تضع استخدامات الذكاء

(١) حميدي، علاء الدين. (٢٠٢٥). الذكاء الاصطناعي وأخلاقياته: تحديات المستقبل القريب. متوفر بالرابط الاتي: https://www.aljazeera.net تاريخ الدخول ٢٤/١١/٢٠٢٥م.

الاصطناعي في مسوغ قانوني حتى يسهل معه تحديد الأبعاد الأخلاقية كالمساءلة والشفافية والخصوصية، كما أنها لم تضع ضوابط تنظيمية للامتثال الفعلي لها، ما يؤثر سلباً على المؤسسات والمنظمات، بما فيها المنظومة القضائية في مكافحة الجرائم التقليدية والإلكترونية، والتي أتاحت تقدير سلطة القاضي في حالة الجرائم الإلكترونية، مما يتير ثغرات قانونية قد تُستغل بطريقة سلبية.

٧. تحديات الهجمات السيبرانية:

يمثل الهجوم السيبراني على تقنية الذكاء الاصطناعي خطراً وتحدياً لتطبيق الذكاء الاصطناعي الذي يعتمد على البيانات وسريتها، ويؤدي التفاعل الواسع مع هذه التقنية إلى إمكانية الهجوم عليها، ومخاطر الوصول غير المصرح به[١]، وبينما يعزز الذكاء الاصطناعي القدرات الدفاعية في مواجهة الجرائم الإلكترونية، إلا أنه يوفر أيضاً أدوات قوية للمهاجمين السيبرانيين، مما يجعلهم يشنون هجمات أكثر تطوراً وتعقيداً، ومنها[٢]:

- هجمات التصيد الاحتيالي المتطورة:

يمكن لهذه الهجمات من تحليل الملفات الشخصية للضحايا على وسائل التواصل الاجتماعي، والبريد الإلكتروني، بحيث تنشأ رسائل تبدو وكأنها موثوقة تتضمن تفاصيل شخصية يمكن تستخدم للنقر على روابط ضارة.

- البرمجيات الخبيثة ذاتية التطور:

يمكن للذكاء الاصطناعي أن يُمكن البرمجيات الخبيثة من التكيف والتطور، بحيث تستطيع تغيير سلوكها وأنماطها للتحايل على أنظمة الدفاع، كأن يتم تطوير فيروسات أو برامج فدية.

- الاستغلال التلقائي للثغرات:

يمكن لهذه الهجمات أتمتة عملية البحث عن الثغرات الأمنية واستغلالها.

---

(١) الهيئة السعودية للبيانات والذكاء الاصطناعي. (٢٠٢٥)، مرجع سابق. ص٦٠.

(٢) السعودي، عبدالعزيز عبدالله. (٢٠٢٥). الذكاء الاصطناعي والأمن السيبراني: سلاح ذو حدين. متوفر بالرابط الآتي: https://wasl.news تاريخ الدخول: ٢٥/١١/٢٠٢٥م.

- الذكاء الاصطناعي العدائي:

تهدف هذه الهجمات على خداع تقنية الذكاء الاصطناعي، مما يجعلها تفشل في الكشف عن التهديدات أو تصدر إنذارات خاطئة.

- التزييف العميق:

هذا النوع لا يمثل هجمات سيبرانية بشكلها التقليدي، إلا أن التزييف العميق المدعوم بالذكاء الاصطناعي يشكل تهديداً أمنياً خطيراً، يمكن استخدامه في التلاعب بالرأي العام وتشويه الحقائق.

الخاتمة

بعد أن استعرضنا ماهية الذكاء الاصطناعي وتطبيقاته، ومعرفة الجرائم الإلكترونية المعاصرة والصور التي تتخذها، وبيان المعوقات التي تواجه الاستفادة من تطبيق الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية، خلصنا إلى الخروج بالنتائج والتوصيات التالية:

أولاً: النتائج:

١. لا يوجد تعريف محدد للذكاء الاصطناعي، حيث لم يستطع الباحثون والعلماء حصر الذكاء الاصطناعي بتعريف موحد، وإنما كل منهم عرفه وفق وظيفته، أو بنائه، أو تكوينه، أو الغرض الذي صُمم من أجله.

٢. بروز جرائم نوعية مصاحبة للتقدم التكنولوجي تعرف بالجرائم الإلكترونية أو السيبرانية، تُرتكب في الفضاء الإلكتروني.

٣. يوفر الذكاء الاصطناعي أساليب حديثة وكفاءة عالية في مواجهة الجرائم الإلكترونية، لذا تسارع الدول إلى الاستفادة القصوى من تقنيات الذكاء الاصطناعي في المجال الأمني والقضائي.

٤. تواجه الأجهزة الأمنية والمنظومة القضائية اليمنية الجرائم الإلكترونية بالأساليب التقليدية، والتي لا تتناسب مع طبيعة هذه الجرائم.

٥. وجود معوقات تواجه تطبيق الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية في اليمن تتمثل في:

- ضعف البنية التحتية.
- نقص الكوادر المتخصصة.
- قصور النصوص التشريعية.
- شحة الموارد المالية.
- تحديات الخصوصية.
- التحديات الأخلاقية.
- الهجمات السيبرانية.

ثانياً: التوصيات:

١. ضرورة مواكبة التقدم التكنولوجي والتقنيات المتميزة والاستفادة من الخدمات التي تقدمها، كتقنية الذكاء الاصطناعي في شتى المجالات.

٢. نوصي بدمج الذكاء الاصطناعي في الأساليب المستخدمة لمواجهة الجرائم الإلكترونية في المجال الأمني والقضائي في اليمن.

٣. نوصي بإقرار مشروع قانون مكافحة جرائم تقنية المعلومات، حتى لا يترك الحكم في الجرائم الإلكترونية لتقدير سلطة القاضي، مما يسهل الطعن فيه، وإضافة جزئية خاصة تتعلق بالذكاء الاصطناعي وتطبيقاته.

٤. نوصي بإنشاء بنية تحتية قوية قائمة على بيانات ضخمة، وتخصيص ميزانية لمواكبة تقنية الذكاء الاصطناعي، مع مراعاة المبادئ الأخلاقية والخصوصية، وتدريب كوادر بشرية لتصميمه واستخدامه قادرة على صد أي هجمات سيبرانية.

٥. نوصي بإدراج مادة الجرائم الإلكترونية والتقنيات الجديدة في منهج المعهد العالي للقضاء اليمني، كخطوة أولى نحو إدراك القضاة ومعاوني النيابة وفهم قضايا الجرائم الإلكترونية المنظورة في المحاكم والنيابات.

المراجع

المراجع العربية

أولاً: المصادر العامة:

١. القرآن الكريم.

٢. القانون اليمني رقم (١٣) لسنة ٢٠١٢م بشأن حق الحصول على المعلومات.

ثانياً: الكتب:

١. إبراهيم، خالد ممدوح. (٢٠٢٢). التنظيم القانوني للذكاء الاصطناعي. دار الفكر القانوني، الإسكندرية، مصر.

٢. الحلبي، خالد عيادي. (٢٠١١). إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت. دار الثقافة، عمان.

٣. الشمري، غانم مرتضى. (٢٠١٦). الجرائم الإلكترونية. الدار العلمية الدولية، عمان، ص٥٣.

٤. الشناوي، محمد. (٢٠٠٧). جرائم الإنترنت وبطائق الائتمان والجريمة المنظمة. دار الكتب الحديثة.

٥. القرعان، محمود أحمد. (٢٠١٧). الجرائم الإلكترونية. دار وائل للنشر والتوزيع، ص١٩.

٦. الكعبي، محمد عبيد. (٢٠٠٩). الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت. دار النهضة العربية، القاهرة، ص٣٣.

٧. محمود، ثائر والعطيات، صادق. (٢٠٠٦). مقدمة في الذكاء الاصطناعي. مكتبة المجتمع العربي للنشر والتوزيع، عمان، الأردن.

ثالثاً: الرسائل العلمية:

١. إبراهيم، علي أحمد. تطبيقات الذكاء الاصطناعي في مواجهة الجرائم الإلكترونية. المجلة القانونية، (٧٥٨-٢٥٣٧).

٢. الأخنش، أمينة والعيداني، محمد. (٢٠٢٣). الذكاء الاصطناعي كآلية لمجابهة الجريمة الإلكترونية. مجلة القانون والعلوم البيئية، ع(٢).

٣. الإدريسي، عبدالسلام. (٢٠٢٤). حماية الخصوصية أمام تحديات الذكاء الاصطناعي. مجلة الذكاء الاصطناعي والتنمية الإقليمية المستدامة، المغرب، (١-٢١).

٤. البشري، محمد الأمين. (٢٠١١). الأساليب الحديثة للتعامل مع الجرائم المستحدثة من طرف أجهزة العدالة الجنائية. جامعة نائف العربية للعلوم الأمنية. الرياض.

٥. بوحفص، راوية وبوستة، ايمان. (٢٠١٨). الجريمة الإلكترونية في التشريع الجزائري. رسالة ماجستير منشورة، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، (١-٧٠).

٦. خليفة، محمد محمد طه. (٢٠١٨). الذكاء الاصطناعي في ميزان التشريع. مجلة دبي القانونية، (١-٣٠).

٧. سلطاني، خديجة الكبرى. (٢٠٢٥). الذكاء الاصطناعي مداخله ومفاهيمه وأهم خصائصه وتطبيقاته في المعالجة الآلية للغة العربية. مجلة جسور المعرفة، ١١(١).

٨. الشاعر، سعود عبدالقادر. (٢٠٢٠). دور الذكاء الاصطناعي في تفعيل إجراءات التحقيق الجنائي في الجرائم الإلكترونية: دراسة مقارنة. رسالة منشورة كلية القانون، جامعة عجمان، الإمارات العربية المتحدة. (١-٣٦).

٩. الشهري، البراء جمعان محمد. (٢٠٢٤). استخدامات تقنيات الذكاء الاصطناعي في مكافحة الجريمة. المجلة العربية للنشر العلمي، ع(٦٨)، (٧٣-٩٢)

١٠. الصحفي، روان بنت عطية الله. (٢٠٢٠). الجرائم السيبرانية. المجلة الإلكترونية الشاملة متعددة التخصصات ع(٢٤)، (١-٥٣).

١١. ضيف الله، زينب. (٢٠٢٣). الذكاء الاصطناعي والقانون. مجلة القانون والعلوم البيئية، مج(٢)، ع(٣).

١٢. العباسي، ميسون بشير والجرجري، فارس علي. (٢٠٢٥). الذكاء الاصطناعي وحجيته في الإثبات المدني: دراسة مقارنة. مجلة كلية القانون للعلوم القانونية والسياسية، ١٤(٥٣)، (٦٠٨-٦٣٤).

١٣. عبداللطيف، عبدالرؤوف وخذيري، عفاف. (٢٠٢٢). مكافحة الجريمة الإلكترونية

في التشريع الجزائري. رسالة ماجستير منشورة من كلية الحقوق والعلوم السياسية، جامعة الشيخ العربي التبسي، الجزائر، (١-١٠١).

١٤. عبدالمحسن، محمد، آل سعد، سعود الشافي والبويدي، بندر عبدالله. (٢٠٢٥). دور الذكاء الاصطناعي في مكافحة الجريمة باستخدام التقنيات التكنولوجية الحديثة. المجلة العلمية، كلية الشريعة والقانون، أسيوط، جامعة الأزهر، مصر، ع(٣٧)، (٥١٩-٥٥٩).

١٥. عبدالنور، عبدالحق وحماس، عمر. (٢٠٢٤). الذكاء الاصطناعي بين ارتكاب الجرائم المالية والوقاية منها. مجلة العلوم القانونية والاجتماعية، ٩(٣)، (٤٨٨-٥٠٨).

١٦. غازي، مهند سعد. (٢٠٢٤). دور الذكاء الاصطناعي في تطوير عمل المنظومة الأمنية. جامعة المنصورة، كلية الحقوق، قسم القانون الجنائي، مصر، ص٦.

١٧. المائل، عبدالسلام، الشربجي، عادل وقابوسة، علي. (٢٠١٩). الجريمة الإلكترونية في الفضاء الإلكتروني. مجلة آفاق للدراسات السياسية والدولية، المركز الجامعي إيليزي ٢٦٠٢-٦٥٤٦ ISNN، (٢٤٢-٢٥٥).

رابعاً: التقارير والمؤتمرات والدوريات:

١. حسن، عفاف عبدالله الحاج وقشوط، أحمد رمضان. (٢٠٢٤). الطبيعة القانونية للذكاء الاصطناعي: دراسة تحليلية في القانون المدني الليبي. المؤتمر العلمي الثاني، لطلاب المرحلة الجامعية والدراسات العليا، الجامعة الأسمرية الإسلامية، (١٢٧-١٤٣).

٢. شادي، عبدالوهاب، الغيظاني، إبراهيم ويحيى سارة. (٢٠١٨). فرص وتهديدات الذكاء الاصطناعي في العشر سنوات القادمة، تقرير المستقبل، ملحق يصدر مع «اتجاهات الأحداث»، ع(٢٧).

٣. عاقلي، فضيلة. (٢٠١٧). الجريمة الإلكترونية وإجراءات مواجهتها في التشريع الجزائري. المؤتمر الدولي الرابع عشر حول الجريمة الإلكترونية، طرابلس.

٤. مرعي، إسراء جبريل رشاد. (٢٠١٦). الجرائم الإلكترونية: الأهداف- الأسباب- طرق الجريمة ومعالجتها. المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، متوفر على الرابط .https://democraticac

de/?p=35426 تاريخ الدخول: ١٣/١١/٢٠٢٥م.

٥. مركز هاردو لدعم التعبير الرقمي. (٢٠١٤). الجريمة الإلكترونية وحجية الدليل الرقمي في الإثبات الجنائي. القاهرة، (١-٤٠).

٦. الهيئة السعودية للبيانات والذكاء الاصطناعي. (٢٠٢٤). تبني أنظمة الذكاء الاصطناعي. الطبعة الثانية.

٧. الهيئة السعودية للبيانات والذكاء الاصطناعي. (٢٠٢٥). الذكاء الاصطناعي التوكلي، تقنياته وتطبيقاته الوطنية. (١-٨٢).

٨. وزارة العدل الكويتية. (٢٠١٨). الجرائم الإلكترونية. معهد الكويت للدراسات القضائية والقانونية، الكويت.

خامساً: المواقع الإلكترونية:

١. حميدي، علاء الدين. (٢٠٢٥). الذكاء الاصطناعي وأخلاقياته: تحديات المستقبل القريب. متوفر بالرابط الآتي: https://www.aljazeera.net تاريخ الدخول ٢٤/١١/٢٠٢٥م.

٢. خليفة، إيهاب. (٢٠١٧). تأثيرات تزايد دور التقنيات الذكية في الحياة اليومية للبشر. مقالة منشورة في الرابط: https://futureuae.com/media تاريخ الدخول ١٠/١١/٢٠٢٥م.

٣. السعودي، عبدالعزيز عبدالله. (٢٠٢٥). الذكاء الاصطناعي والأمن السيبراني: سلاح ذو حدين. متوفر بالرابط الآتي: https://wasl.news تاريخ الدخول ٢٤/١١/٢٠٢٥م.

٤. الموقع الرسمي لشركة IBM عبر الرابط: https://www.ibm.com/sa-ar/think/topics/ai-infrastructure تاريخ الدخول: ٢٢/١١/٢٠٢٥م.

المراجع الأجنبية

1. Deloitte. Insghts. Development Under: agents AI generative A:. (Deloitte. Insghts. 2024).