AL-NAHRAIN JOURNAL OF LEGAL SCIENCE Vol.27 2025, pp. 206-219

AL-NAHRAIN UNIVERSITY
COLLEGE OF LAW

ISSN:3006- 0605 DOI:10.58255

عدد: مؤتمر (الفراهيدي) المجلد: ٢٧ تموز ٢٠٢٥ مجلة النهرين للعلوم القانونية

Received:1/3/2025 Accepted: 7/4/2025 Published: 1/6/2025

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0)

Digital Guardian: The Relationship Between Artificial Intelligence and Crime: Positives and Negatives

Abdul Karim Adnan Ashraf

Al-Farahidi University - College of Law

Abstract

Artificial intelligence (AI) is a double-edged tool in the field of crime. On the one hand, it contributes to crime prevention through predictive analytics systems that identify potential crime hotspots, facial recognition technologies in security surveillance, and financial fraud detection tools. It also enhances criminal investigations through the analysis of big data and the rapid and accurate tracking of digital evidence. On the other hand, AI is used in the commission of crimes, such as sophisticated cyberattacks using self-learning algorithms, identity theft through deepfake technologies, and the development of intelligent malware. It also facilitates automation in traditional crimes, such as the use of robots in pickpocketing or smuggling operations.

This relationship highlights ethical and legal challenges, such as privacy breaches and algorithmic bias, which require the development of flexible legislative frameworks and advanced security technologies to enhance AI's positive role in criminal justice while limiting its misuse.

الحارس الرقمي العلاقة ما بين الذكاء الاصطناعي و الجريمة السلبيات و الايجابيات

م . م عبد الكريم عدنان اشرف
مدرس مساعد القانون الجنائي
جامعة الفراهيدي – كلية القانون
Abdulkareem.Adnan1203a@colaw.uobaghdad.edu.iq
٠٧٧٠٩٤١١٤٩٦

المستخلص
يُعد الذكاء الاصطناعي (AI) أداة ذات حدين في مجال الجريمة، فمن ناحية، يُسهم في منع الجريمة من خلال أنظمة التحليل التنبؤي التي تُحدد بؤر الجريمة المحتملة، وتقنيات التعرف على الوجوه في المراقبة الأمنية، وأدوات كشف الاحتيال المالي. كما يُعزز التحقيقات الجنائية عبر تحليل البيانات الضخمة وتتبع الأدلة الرقمية بسرعة ودقة. ومن ناحية أخرى، يُستخدم الذكاء الاصطناعي في ارتكاب الجريمة، مثل الهجمات الإلكترونية المتطورة باستخدام خوارزميات ذاتية التعلُّم، وانتحال الهوية عبر تقنيات التزييف العميق (Deepfake)، وتطوير برمجيات ضارة ذكية. كذلك، يُسهِّل الأتمتةَ في الجرائم التقليدية، مثل استخدام الروبوتات في عمليات النشل أو التهريب.
تُبرز هذه العلاقة التحديات الأخلاقية والقانونية، مثل اختراق الخصوصية أو التحيز في الخوارزميات، مما يتطلب تطوير أطر تشريعية مرنة وتقنيات أمنية متقدمة لتعزيز دور الذكاء الاصطناعي الإيجابي في العدالة الجنائية، مع الحد من إساءة استخدامه.

المقدمة :

في الآونة الاخيرة يشهد عصرنا الحالي تطورا ملحوظا في مجال التكنلوجيا و المعلومات على شتى المجالات ومن احد نماذج هذا التطور التكنلوجي هو ظهور عصر الذكاء الاصطناعي الذي استطاع خلال فترة وجيزة ان يحتل اهمية كبيرة في المجتمع وفي مختلف المجالات ، كما ان لهذا التطور دورا ايجابيا في خدمة المجتمع فأن له ايضا سلبيات ومن هذه السلبيات هو استخدام الذكاء الاصطناعي في ارتكاب الجرائم عامة،إذ ان مع تطور التكنلوجيا اصبح المجرمون يستغلون هذا التطور في ارتكاب جرائم اكثر تعقيدا و تطورا وذلك مما يشكل انذارا بخطر كبير يواجهه المجتمع و اهمية هذا الخطر تكمن في صعوبة معرفته وكشفه ، وعليه على الرغم من ان الذكاء الاصطناعي يقدم فوائد هائلة في مجالات الطب و الصناعه و الأمن إلا ان اساءة استعماله بسوء قصد ممكن ان يقود الى ارتكاب جرائم خطيرة و معقدة

اهمية البحث :

بالنظر للتطور الكبير الذي يشهده عالمنا في مجال العلم و الرقميات فلا بد من البحث عن العلاقة بين الذكاء الاصطناعي و الجريمة بمختلف انواعها الواقعية و الالكترونية من جانبين احدهما ايجابي و الاخر سلبي ،، فمن حيث الجانب الايجابي هو وسيلة للحماية منها اما الجانب السلبي فهو وسيلة ارتكابها وبالتالي يتيح لنا فهم تأثير هذه التكنلوجيا على هذه الجريمة بالذات و ايجاد الحلول للحد من انتشارها و التوعية بخطورة هذا الامر.

هدف البحث :

إن بحثنا يهدف الى التعريف بالذكاء الاصطناعي وعلاقته بالجريمة من خلال بيان طريقة استخدامه من الناحية الايجابية المتمثلة بالكشف عن الجريمة المرتكبة بواسطته او من خلال دوره السلبي في استخدامه وسيلةً في ارتكابها وذلك لغرض المساهمة في حماية الافراد من الاثار السلبية للجريمة بواسطة الذكاء الاصطناعي إذ تكون هذه الآثار كبيرة بسبب صعوبة اكتشاف ان الفعل المجرم قد ارتكب بواسطة الذكاء الاصطناعي .

اشكالية البحث :

تدور اشكاليات البحث الأساسية حول البحث مدى استخدام الذكاء الاصطناعي في ارتكاب الجريمة وصعوبة اكتشافها و سبل مواجهتها .

هيكلية البحث :

سيتم تقسيم البحث على مبحثين

المبحث الاول : التعريف بالذكاء الاصطناعي و الجريمة

المبحث الثاني : طبيعة الذكاء الاصطناعي و دوره في الجريمة

المبحث الاول
التعريف بالذكاء الاصطناعي و الجريمة

لغرض بيان العلاقة ما بين الذكاء الاصطناعي و الجريمة يتطلب منّا في بداية الامر بيان ما هو الذكاء الاصطناعي ومن ثَمَّ بيان الجريمة حتى يتسنى لنا تحديد ماهية العلاقة المتواجدة بينهم ، وبناء على ما تقدم سنقسم مبحثنا الى مطلبين حيث نخصص الاول لبيان الذكاء الاصطناعي ومميزاته، بينما يكون المطلب الثاني مخصص لبحث الجريمة من حيث التعريف و الانواع

المطلب الاول
ماهية الذكاء الاصطناعي

لاجل بيان ماهية الذكاء الاصطناعي و الجريمة سنقسم هذا المطلب الى فرعين حيث نخصص الفرع الاول لبيان ما هو الذكاء الاصطناعي بينما يكون الثاني مخصص لبيان مميزات الذكاء الاصطناعي.

الفرع الاول
ماهية الذكاء الاصطناعي

لغرض بيان وفهم ماهية الذكاء الاصطناعي يوجب علينا تعريف الذكاء الاصطناعي

اولا : التعريف بالذكاء الاصطناعي

يمثل الذكاء الاصطناعي أحد أهم وأخطر إفرازات الثورة الصناعية الرابعة التي توهجت في العصر الرقمي نتيجة لما انبثق عنها من تطبيقات ذكية أثرت على مختلف مناحي الحياة ، وأسهمت في خدمة البشرية والارتقاء بها من خلال علم هندسة الآلات الذكية التي تقوم على إنشاء أجهزة وبرامج كمبيوتر قادرة على التفكير بالطريقة التي يعمل بها الدماغ البشري[١]، والتي مكّنت الذكاء الاصطناعي Artificial Intelligence من تقديم نسخة إلكترونية مشابهة للإنسان ولديها القدرة على التعلم باكتساب المعلومات والقدرة على تحليل البيانات والمعلومات والقدرة على إيجاد العلاقات، ومن ثَمَّ يكون لديها القدرة على اتخاذ القرار السليم لإظهار ردود الفعل المناسبة للمواقف التي تتعرض لها الآلة الإلكترونية واستغلالها في تحقيق المهمة التي تكلف بها[٢].

يُعد الذكاء الاصطناعي أحد أهم التقنيات في العصر الرقمي، حيث يجمع بين القدرة على تحليل البيانات المعقدة وأتمتة المهام بذكاء. ومع ذلك، فإن استخدامه الأمثل يتطلب موازنة بين الابتكار وإدارة المخاطر الأخلاقية والاجتماعية ، ولذلك يعرف الذكاء الاصطناعي بأنه فرعٌ من علوم الحاسوب يهدف إلى تطوير أنظمة قادرة على أداء مهام تتطلب ذكاءً [٣]بشرياً، مثل التعلم، التفكير المنطقي، التحليل، فهم اللغة، والإدراك. تُبنى هذه الأنظمة على خوارزميات تُمكّن الآلات من معالجة البيانات، التعلم من التجارب، واتخاذ قرارات بدرجة من الاستقلالية.

وهناك من يعرفه بأنه "نظام قائم على البرمجيات أو الأجهزة، مصمم لاتخاذ قرارات وتنبؤات أو توصيات تؤثر على البيئات المادية أو الرقمية[٤]".

ويعرف ايضا بأنه "القدرة التقنية للآلات على محاكاة الوظائف المعرفية البشرية، مثل الإدراك والتعلم وحل المشكلات"[٥].

---

(١) اروى عبد الرحمن بن عمثان ،احكام تطبيقات الذكاء الاصطناعي في القضاء ، الطبعة الأولى ، ص ٣٣ د.فايق عوضين محمد ، استخدامات الذكاء الاصطناعي بين المشروعية وعدم المشروعية ،مجلة المركز القومي للبحوث الاجتماعية ، مجلد ٦٤ ، عام ٢٠٢١

(٢) خالد ناصر . أصول الذكاء الصناعي . (الرياض ، مكتبة الرشد ، الطبعة الاولى ، ٢٠٠٤م

(٣) محمد سعد الدين محمد ، الذكاء الاصطناعي و الحياة في عام ٢٠٣٠ ، مركز المستقبل ، العدد ٣٠٣ ، ٢٠١٧ ، ص ٢

(٤) زياد عبد الكريم القاضي ، مقدمة في الذكاء الاصطناعي ،ط١، دار الصفاء للطباعة و التشر والتوزيع ، ٢٠١٠ ، ص٢٥

الفرع الثاني
مميزات الذكاء الاصطناعي

تمتع الذكاء الاصطناعي (AI) بمجموعة فريدة من المزايا التي تجعله أداة تحويلية في مختلف المجالات، بما في ذلك النظام القانوني والقطاع الأمني. هذه المميزات لا تقتصر على الجانب التقني فحسب، بل تمتد لتشمل تأثيرات اجتماعية واقتصادية وقانونية عميقة، تمثل مميزات الذكاء الاصطناعي قفزة نوعية في العمل القانوني والقضائي، لكنها تتطلب إطاراً تنظيمياً متكاملاً لضمان الاستخدام الأمثل. التشريعات الذكية والبنية التحتية المناسبة والملاكات المؤهلة تشكل ثلاثية النجاح لاستثمار هذه الإمكانات وعلى ذلك نبين اهم مميزاته

ان من اهم مميزات الذكاء الاصطناعي هي[١] : -

١. التصدي للجرائم الرقمية تحليل أنماط الجرائم الإلكترونية عبر التعلم العميق لاساليب الجريمة الالكترونية
٢. الأمن السيبراني المعزز الحماية الاستباقية أنظمة Darktrace تكشف التهديدات الأمنية قبل وقوعها.
٣. لكشف عن الأنماط الخفية من خلال تحديد الروابط غير المرئية في قضايا غسل الأموال مثل نظام FINSense التابع للإنتربول يكشف المعاملات المشبوهة بدقة ٩٢%
٤. التعلم الآلي (Machine Learning) يمكن للأنظمة تحسين أدائها تلقائياً من خلال تحليل البيانات دون برمجة صريحة، مثل أنظمة التوصية في Netflix أو Amazon التي تتعلم من سلوك المستخدم.
٥. معالجة اللغة الطبيعية (NLP) فهم وتوليد اللغة البشرية، مما يُستخدم في المساعدات الصوتية المتوافرة على اجهزة الموبايل (مثل Siri وChatGPT).
٦. الرؤية الحاسوبية (Computer Vision) تحليل الصور والفيديوهات، مثل التعرف على الوجوه في أنظمة المراقبة أو السيارات ذاتية القيادة كما هو معمول في كاميرات مراقبة السرعة[٢] .
٧. التشخيص الطبي الدقيق تحليل البيانات الطبية للكشف عن الأمراض بدقة عالية، مثل تشخيص السرطان من خلال الصور الإشعاعية وبالتالي يلعب الذكاء الاصطناعي دورا كبيرا في مجال الطب[٣] .
٨. الأتمتة الذكية : بسبب التطور السريع الذي يشهده العالم وكثرة عدد السكان والتحول الرقمي الذي نعيشة يتطلب ادخال كمٍ هائلٍ من المعلومات، وهذا يتطلب وقتا وجهدا وعلى هذا الاساس يلعب الذكاء الاصطناعي دورا في تحسين العمليات الصناعية والخدمية عبر الروبوتات الذكية، مما يقلل الأخطاء البشرية.
٩. التنبؤ بالنتائج تحليل البيانات الضخمة للتنبؤ بما ممكن أن يحدث، مثل توقع الطقس أو أسعار الأسهم أو حتى توقع ارتكاب الجريمة [٤].

---

(١) عبد النور ، عادل . أساسيات الذكاء الاصطناعي . (الرياض ، دار الفيصل الثقافية ، الطبعة الاولى ، ٢٠٠٥م
٢)ايمن محمد الاسيوطي ، الجوانب القانونية لتطبيق الذكاء الاصطناعي ، ط١ ، ٢٠٢٠ ، دار مصر للتوزيع و النشر ، ص ٢٢
(٣) زين عبد الهادي ، الأنظمة الخبيرة للذكاء الاصطناعي ، دار الكتب للنشر و التوزيع ، القاهرة ، ٢٠١٩ ، ص ٦
كرستيان يوسف ، المسؤولية المدنية عن فعل الذكاء الاصطناعي ، رسالة ماجستير مقدمة إلى مجلس كلية الحقوق ، (4) الجامعة اللبنانية ، ٢٠٢٠ ، ص ٢٢

المطلب الثاني
ماهية الجريمة وانواعها

لغرض بيان وفهم ماهية الجريمة يوجب علينا ان نبين اولا تعريف الجريمة ومن ثم تحديد انواع الجرائم لغرض ايجاد العلاقة ما بين الذكاء الاصطناعي و الجريمة وعليها خصصنا الفرع الاول لبيان ماهية الجريمة بينما يكون الثاني مخصص لبيان انواع الجريمة

الفرع الاول
ماهية الجريمة

ان الجريمة عبارة عن ظاهرة اجتماعية تهدد امن المجتمع موجودة منذ الازل وقد اخذت الدول على عاتقها مكافحتها، إذ سنّت القوانين مبينة فيها الجرائم و محددة الاجراءات و التدابير و العقوبات المناسبة لها لغرض الحد منها[١] ، وعلى الرغم من ذلك جاءت غالبية قوانين العقوبات الحديثة خالية من تعريف الجريمة وهذا مسلك محمود لان وضع تعريف محدد للجريمة يقيد من نطاق العدالة لان مهما كان التعريف جامعا لكل المعاني المطلوبة في زمن معين، لكنه لن يكون ذا فائدةٍ في زمن آخر وعلى هذا الاساس تبنى المشرع مبدأ قانونية الجرائم و العقوبات، إذ وضع لكل جريمة نصا خاصا يبين اركانها و العقوبات المحددة لها ومن هذه القوانين قانون العقوبات العراقي لكن يمكن ان نستشف تعريف الجريمة من خلال بعض نصوص قانون العقوبات هي كل فعل أو امتناع عن فعل يُجرّمه القانون ويقرر له عقوبة، سواء كان هذا الفعل مادياً أو معنوياً[٢].

ويعرفها الفقه القانوني بأنها: من الناحية القانونية: "كل انتهاك للقوانين الجنائية يُعاقب عليه بالعقوبات المقررة" (مثل السجن أو الغرامة) ، و من الناحية الاجتماعية: "سلوك منحرف يهدد أمن المجتمع واستقراره"[٣].

وللجريمة أركان الأساسية متمثلة بالركن المادي (السلوك الإجرامي والنتيجة والعلاقة السببية) الفعل أو الامتناع الذي ينتهك القانون والنتيجة الاجرامية والعلاقة السببية التي تربط بينهم ، و الركن المعنوي (القصد الجنائي في الجرائم العمدية و الخطا الغير العمدي في الجرائم الغير عمدية) ، واخيرا الركن الشرعي (النص القانوني): وجود نص قانوني يجرم الفعل[٤].

وهناك أنواع الجرائم التقليدية: جرائم ضد الأشخاص (مثل القتل، الاعتداء)، وجرائم ضد المال (مثل السرقة، الاحتيال)، و جرائم ضد الأخلاق (مثل الابتزاز، الاعتداء الجنسي)، و جرائم ضد الدولة (مثل الخيانة العظمى، التخريب).

الفرع الثاني
انواع الجرائم

تقسم الجرائم الى عدة انواع حسب معايير مختلفة مثلا تقسم الى جريمة عمدية وغير عمدية بواسطة معيار الركن المعنوي وكذلك تقسم جرائم ايجابية وسلبية حسب مظهر السلوك ولكن الذي يهمنا في هذا البحث هو تقسيم الجرائم الى جرائم مادية و جرائم الكترونية استنادا الى طبيعة السلوك حيث كانت في العالم الحقيقي او في العالم الافتراضي.

إذ شهد العالم خلال العقود الاربع المنصرفة تطوراً علمياً كبيراً كان من ابرز ملامحة ما اطلق علية ب(الثورة التكنولوجية) والتي أسفرت عن الغزو التقني في كافة نواحي الحياة حيث أصبحت الادوات والوسائل الالكترونية امراً لا غنى عنه في المؤسسات الحكومية والخاصة وكذلك لدى الافراد في المجتمع كما أصبح الغالبية العظمى لديهم المهارة والقدرة على استخدام تلك الادوات

---

(١)علي حسين خلف و سلطان الشاوي ، المبادئ العامة في قانون العقوبات ، المكتبة القانونية ، ٢٠٠٨ ، ص ١٧٨
(٢) جمال ابراهيم الحيدري ، الوافي في شرح قانون العقوبات القسم العام ، مكتبة السنهوري ، ٢٠٠٧ ، ص ٣٤
(٣) علي حسين خلف و سلطان الشاوي ، مصد سابق ، ص١٨٠
(٤)محمود نجيب حسني ، شرح المبادئ العامة في قانون العقوبات ، دار النهضة العربية ، ١٩٨٨، ص ٧٦

والتعامل معها بكفاءة عالية مما أدى ذلك الى بروز نوعية جديدة من الجرائم سميت ب(الجرائم الالكترونية)([1]

وتُعد الجرائم الالكترونية من الجرائم التي ثبتت مسمياتها خلال المراحل الزمنية لتطورها. التي ارتبطت بتقنية المعلومات فقد أصطلح على تسميتها في البداية باسم اساءة استخدام الكمبيوتر واحتيال الكمبيوتر

ونلاحظ ثمة اتجاهات تضيف مفهوم الجريمة الالكترونية ومن هذه التعريفات هو ما يحصر الجريمة المعلوماتية في الاموال التي تحتاج الى قدرٍ كبيرٍ من المعارف التقنية في ارتباكها وهو ما تحقق في بعضها الاحوال فأنه لا يتحقق في كثير منها ففي بعضها الاحوال يرتكب الفعل من دون الحاجة الى هذا القدر من المعرفة ورغم ذلك لا يمكننا انكار ايّ من هذه الافعال التي تدخل في اعداد الجرائم الالكترونية ولا يعرف البعض جريمة الحاسوب بأنها نشاط غير مشروع موجه لنسخ او تغير او حذف او الوصول الى المعلومات المخزنة داخل الحاسب الآلي او تلك التي يتم تحويلها عن طريقه ، ومن هذه الاتجاهات أيضاً الاتجاه الموسع للجريمة الالكترونية ويكون هذا الاتجاه عكس الاتجاه السابق فيذهب بعضها الفقهاء الى تعريف الجريمة الالكترونية بأنها سلوك اجرامي يتم لمساعدة الحاسب الآلي او هي كل جريمة تتم في محيط الحاسوب الآلي، ذهبوا الى تعريف الجريمة المعلوماتية بأنها سلوك غير مشروع او غير اخلاقي او غير مصرح به تتعلق لمعالجة الآنية للبيانات او نقلها[2] .

نظراً لارتباط الجريمة الالكترونية بجهاز الحاسوب ، وشبكة الانترنت بصورة عامة ووسائل التواصل الاجتماعي بصورة خاصة فلقد أخفى عليها مجموعة من الخصائص المميزة لها التي تجعلها غير الجرائم التقليدية ومن هذه الخصائص في انها جرائم عابرة للحدود، إذ من السهولة بفعل ربط الحواسيب بالشبكة العنكبوتية ان يكون الجاني في دولة والمجني علية في دولة اخرى وهنا تظهر الحاجة لوجود تنظيم قانوني دولي وداخلي متلائم معهُ لمكافحة هذه الجرائم مع الاشارة الى ان التوجيهات الداخلية في قوانين الدول متفاوتة في مناقشة هذا الموضوع هنا تظهر مشاكل في تحديد الجهة المختصة قضائياً في نظر هذه القضايا مع ذكر ان جرائم الانترنيت في هذه الخاصية تشابه مع جرائم غسيل الاموال وجرائم المخدرات من خصائصها ايضا انها جريمة صعبة الاثبات والاكتشاف والسبب في ذلك لانها لا تترك ايّ اثرٍ ماديّ ظاهرٍ يمكن ضبطه، فضلاً عن التباعد الجغرافي الذي يثير الاشكال بداية؛إذ تشير الدراسات الى ان ما تم اكتشافه من جرائم المعلومات يصل الى نسبة ١% والذي يتم الابلاغ عن هذه النسبة لا يكاد يصل الى ٥%فقط ، والوسيلة المستخدمة لارتكاب الجريمة هي سبقة الكترونية ينتهي دورها في اقل من ثانية واحدة وكأن الجاني يقوم بتدمير كل دليل لمجرد الاستعمال وبكل هدوء من دون أيّ ضجة.

(1) جمال الحيدري ، الجرائم الالكترونية وسبل معالجتها ، مكتبة السنهوري ، ٢٠١٢ ، ص ٥٥

(2) جمال الحيدري ، الجرائم الالكترونية وسبل معالجتها ، مكتبة السنهوري ، ٢٠١٢ ، ص ٣٤

المبحث الثاني
ماهية العلاقة ما بين الذكاء الاصطناعي و الجريمة

يشهد العصر الرقمي تحولاً جوهرياً في طبيعة الجريمة وأساليب مكافحتها ،إذ أصبح الذكاء الاصطناعي (AI) عاملاً محورياً في هذه المعادلة. تُعتبر هذه العلاقة ثنائية الاتجاه: فبينما يُسهم الذكاء الاصطناعي في تطوير أساليب إجرامية غير مسبوقة، فإنه أيضاً يُشكّل أداة فاعلة في يد الأجهزة الأمنية والقضائية لمكافحة الجريمة

و يُشكّل الذكاء الاصطناعي (AI) تحولاً جذرياً في مختلف المجالات، بما في ذلك عالم الجريمة والأمن. فبينما يُسهم في تطوير أساليب جديدة لارتكاب الجرائم، فإنه أيضاً يُعد أداة فاعلة في مكافحتها. وتكمن إشكالية العلاقة بين الذكاء الاصطناعي والجريمة في كونه سيفاً ذا حدين: أداة للخطر وأداة للحماية في آن واحد. . من خلال هذا البحث نقدم تحليلاً قانونياً شاملاً لهذه العلاقة، مع التركيز على الجرائم الإلكترونية[١].

المطلب الاول
الذكاء الاصطناعي كأداة لارتكاب الجريمة

مع التطور التكنولوجي المتسارع، أصبح الذكاء الاصطناعي (AI) أداة قوية يمكن استخدامها في مجالات متعددة، بما في ذلك المجالات الإجرامية[٢].

ويمكن استخدام تقنيات الذكاء الاصطناعي بشكل ضار لتنفيذ جرائم أكثر تعقيداً وتطوراً، ومن أبرزها الجرائم الإلكترونية المعزَّزة بالذكاء الاصطناعي ،هجمات إلكترونية ذكية تُستخدم خوارزميات التعلم الآلي لاختراق الأنظمة بطرق متطورة، مثل الهجمات التكيُّفية التي تتغير تكتيكاتها تلقائياً لتفادي أنظمة الحماية ، وايضا جريمة التصيد الاحتيالي المتقدم (Phishing): يمكن للذكاء الاصطناعي تحليل بيانات الضحايا لإنشاء رسائل احتيالية مخصصة تبدو أكثر واقعية، مما يزيد من فرص نجاحها.

ومن بين الجرائم التي يمكن أن تسهل التكنولوجيا ارتكابها على سبيل المثال هي جرائم السب والقذف والتنمر الالكتروني. في هذا المطلب، سنناقش كيفية استخدام الذكاء الاصطناعي في ارتكاب هذه الجرائم، والإطار القانوني الذي يحكمها في القانون العراقي

الفرع الاول
مفهوم السب والقذف في التشريع العراقي ودور الذكاء الاصطناعي في ارتكابها

السب والقذف من الجرائم التي تُعد اعتداءً على شرف وكرامة الأشخاص، وتنص عليها المادة ٤٣٣ من القانون الجنائي العراقي. إذ يعتبر السب إهانةً موجهةً لشخصٍ ما، بينما القذف هو اتهام شخص بارتكاب فعل معين دون تقديم أدلة كافية.

ويمكن استخدام الذكاء الاصطناعي بعدة طرق لتسهيل ارتكاب جريمة السب والقذف، ومنها:

١. إنشاء محتوى مزيف: يمكن للذكاء الاصطناعي إنشاء نصوص أو صور أو مقاطع فيديو مزيفة تُظهر شخصاً ما في مواقف مُهينة أو تُنسب إليه أفعالاً لم يرتكبها.
٢. التزييف العميق (Deepfake): تقنية Deepfake تسمح بإنشاء مقاطع فيديو تبدو حقيقية لشخص ما وهو يقول أو يفعل أشياء لم تحدث، مما يمكن استخدامه للقذف أو السب.

---

(١) الهادي محمد محمد . الجريمة الالكترونية عبر شبكة الانترنت . (القاهرة ، الدار المصرية اللبنانية ، الطبعة الاولى ، ٢٠٠٥م)

(٢) عادل حافظ غانم ، الوسائل العلمية الحديثة لكشف الجريمة ومشروعيتها وحجيتها ، المجلة العربية للدفاع الاجتماعي ، عدد الرابع ، ٢٠٠٦، ص ٢٣

٣. الروبوتات والبرامج الآلية: يمكن استخدام برامج الذكاء الاصطناعي لنشر اتهامات أو إهانات بشكل واسع عبر وسائل التواصل الاجتماعي، مما يزيد من انتشار الجريمة ويصعب تتبع مصدرها.

في القانون العراقي، لا توجد نصوص قانونية محددة تتناول استخدام الذكاء الاصطناعي في ارتكاب الجرائم بشكل عام، أو جرائم السب والقذف بشكل خاص. ومع ذلك، يمكن تطبيق النصوص العامة المتعلقة بالسب والقذف على هذه الحالات، حيث أن الجريمة تتحقق بمجرد وقوع الفعل الجرمي بغض النظر عن الوسيلة المستخدمة ، لكن نجد من خلال
نص المادة ٤٣٣ من القانون العقوبات العراقي نصت على عقوبة الحبس أو الغرامة لمن يوجه إهانة أو اتهاماً كاذباً لشخص آخر.
و يمكن أن تتحقق المسؤوليةً الجنائية لمن يستخدم الذكاء الاصطناعي لارتكاب الجريمة، وكذلك لمطوري البرامج إذا كانوا على علمٍ باستخدامها لأغراض إجرامية[١].
ومن خلال استخدام الذكاء الاصطناعي في جرائم السب و القذف يخلق لدينا مجموعة من العوائق لا نجدها في حال عدم استخدام الذكاء الاصطناعي وعليه من اهمها :

١. صعوبة الإثبات: قد يكون من الصعب إثبات أن المحتوى المزيف تم إنشاؤه باستخدام الذكاء الاصطناعي، ولاسيّما إذا كان المحتوى ذا جودة عالية.
٢. صعوبة تحديد الجاني: في حال استخدام برامج أو روبوتات، قد يكون من الصعب تحديد الشخص المسؤول عن الجريمة.

بناءً على ما تقدم نجد ان استخدام الذكاء الاصطناعي في ارتكاب جرائم السب والقذف يمثل تحدياً جديدًا للقانون العراقي. وعلى الرغم من أن النصوص الحالية يمكن تطبيقها على هذه الجرائم، إلا أن هناك حاجة ماسة لتحديث التشريعات لمواكبة التطورات التكنولوجية وضمان حماية فعالة لحقوق الأفراد.

الفرع الثاني

مفهوم جريمة التنمر في التشريع العراقي ودور الذكاء الاصطناعي في ارتكابها

التنمر هو سلوك عدواني متكرر يهدف إلى إلحاق الأذى النفسي أو الجسدي بالضحية، وقد تطورت أساليب التنمر مع التقدم التكنولوجي ليشمل ما يُعرف بالتنمر الإلكتروني[٢]. ومع ظهور الذكاء الاصطناعي (AI)، أصبحت أدوات التكنولوجيا الحديثة تُستخدم لتعزيز وتسهيل ارتكاب جرائم التنمر. في هذا التقرير، سنناقش كيفية استخدام الذكاء الاصطناعي في ارتكاب جريمة التنمر، والإطار القانوني الذي يحكمها في القانون العراقي.
في العراق، لا يوجد نصٌ قانونيٌّ محدد يتناول جريمة التنمر بشكل مباشر، ولكن يمكن تطبيق نصوص قانونية عامة من القانون الجنائي العراقي على حالات التنمر،ولاسيّما إذا ترتب عليها أذى نفسي أو جسدي للضحية. ومن هذه النصوص نص المادة ٤٢١ من القانون العقوبات العراقي والتي تعاقب على الأفعال التي تسبب أذى جسدياً أو نفسياً للآخرين.

---

(١) وليد سعد الدين محمد ، المسؤولية الجنائية الناشئة عن تطبيقات الذكاء الاصطناعي ، مجلة العلوم القانونية ، جامعة عين شمس -كلية الحقوق ، ٢٠٢٢ ، ص ٤٠
(٢)سحر فؤاد مجيد ، جريمة التنمر الالكتروني (دراسة في القانون العراقي الامريكي)، المجلة الاكاديمية للبحث القانوني ، المجلد ١١ ، العدد الرابع ، ٢٠٢٤،ص١٣٥

ومن خلال ربط جريمة التنمر بالذكاء الاصطناعي فأنه يمكن استخدام الذكاء الاصطناعي بعدة طرق لتسهيل ارتكاب جريمة التنمر، ومنها[١]:

١. إنشاء محتوى مسيء: يمكن للذكاء الاصطناعي إنشاء نصوص أو صور أو مقاطع فيديو مسيئة تُستخدم لمهاجمة الضحية بشكل متكرر ومنسق.
٢. الروبوتات والبرامج الآلية: يمكن استخدام برامج الذكاء الاصطناعي لإرسال رسائل تنمر بشكل متكرر عبر وسائل التواصل الاجتماعي أو البريد الإلكتروني، مما يزيد من تأثير التنمر على الضحية.
٣. التزييف العميق (Deepfake): يمكن استخدام تقنيات الذكاء الاصطناعي لإنشاء مقاطع فيديو أو صور مزيفة تُظهر الضحية في مواقف مُهينة أو مُحرجة، مما يعزز من تأثير التنمر.

في القانون العراقي، لا توجد نصوص قانونية محددة تتناول استخدام الذكاء الاصطناعي في ارتكاب جرائم التنمر. ومع ذلك، يمكن تطبيق النصوص العامة المتعلقة بالأذى النفسي والجسدي على هذه الحالات.

١. المادة ٤٢١ من القانون العقوبات العراقي: تنص على عقوبة الحبس أو الغرامة لمن يتسبب في أذى جسدي أو نفسي للآخرين.
٢. المادة ٤٣٣ الخاصة بالسب والقذف: يمكن تطبيقها إذا تضمن التنمر إهانات أو اتهامات كاذبة.

حيث تتحقق المسؤولية الجنائية لمن يستخدم الذكاء الاصطناعي لارتكاب التنمر، وكذلك لمطوري البرامج إذا كانوا على علمٍ باستخدامها لأغراض إجرامية ، ومن خلال استخدام الذكاء الاصطناعي في جرائم التنمر الالكتروني يخلق لدينا مجموعة من العوائق لا نجدها في حال عدم استخدام الذكاء الاصطناعي وعليه من اهمها[٢] :

١. صعوبة الإثبات: قد يكون من الصعب إثبات أن المحتوى المسيء تم إنشاؤه باستخدام الذكاء الاصطناعي،زلاسيّما إذا كان المحتوى ذا جودة عالية.
٢. صعوبة تحديد الجاني: في حال استخدام برامج أو روبوتات، قد يكون من الصعب تحديد الشخص المسؤول عن التنمر.

وبناءً على ما تقدم نرى انه يحتاج القانون العراقي إلى تحديث لتشمل نصوصه جرائم التكنولوجيا الحديثة، بما في ذلك استخدام الذكاء الاصطناعي في ارتكاب التنمر، حيث ان استخدام الذكاء الاصطناعي في ارتكاب جرائم التنمر يمثل تحدياً جديداً للقانون العراقي. وعلى الرغم من أن النصوص الحالية يمكن تطبيقها على هذه الجرائم، إلا أن هناك حاجة ماسة لتحديث التشريعات لمواكبة التطورات التكنولوجية وضمان حماية فعالة لحقوق الأفراد.

---

(١) سحر فؤاد مجيد ، الجرائم المستحدثة (درسة معمقة ومقارنة في عدة جرائم) ، المركز العربي للنشر و التوزيع ، القاهرة ، ط١ ، ٢٠١٩ ، ص ١٢٥

(٢) يحيى ابراهيم دهشان ، المسؤولية الجنائية في جرائم الذكاء الاصطناعي ، ٢٠١٩، ص ٦

المطلب الثاني

الذكاء الاصطناعي بوصفه أداةً لمنع ارتكاب الجريمة

أصبح الذكاء الاصطناعي (AI) أداةً فعالةً في العديد من المجالات، بما في ذلك مكافحة الجريمة. يتمتع الذكاء الاصطناعي بالقدرة على تحليل كميات هائلة من البيانات، والتنبؤ بالسلوك الإجرامي، وتحسين عمليات التحقيق والمراقبة ، سنتكلم عن دور الذكاء الاصطناعي في مواجهة الجريمة بصورة عامة في الفرع الاول، بينما يكون الفرع الثاني مخصص لبيان دور الذكاء الاصطناعي في مواجهة جرائم السب والقذف والتنمر الالكتروني

الفرع الاول

دور الذكاء الاصطناعي في مواجهة الجرائم عامة

كل تقدم علمي يشهده العالم يكون له جانبين سلبي و ايجابي فأن ظهور الذكاء الاصطناعي يمكن ان يكون له جانب سلبي ويتمثل بوصفه أداةً او وسيلةً لتسهيل ارتكاب الجريمة لكن في الوقت نفسه له جانب ايجابي وهو إمكانية استخدامه حارساً رقمياً لمنع ارتكاب الجرائم عامة ومنع ارتكاب بعض الجرائم بصورة خاصة ويمكن تحديد الدور الذي يلعبه الذكاء الاصطناعي بوصفه أداةً تمنع ارتكاب الجريمة من خلال بعض النقاط الاساسية[١] وهي :

١. تحليل البيانات والتنبؤ بالجريمة:

من خلال تحليل الأنماط الإجرامية،إذ يمكن للذكاء الاصطناعي تحليل البيانات التاريخية للجرائم لتحديد الأنماط والاتجاهات الإجرامية. على سبيل المثال، يمكن للخوارزميات التنبؤ بمناطق الجريمة المحتملة بناءً على عوامل مثل الوقت والمكان والظروف الاجتماعية.

٢. الوقاية من الجريمة:

يمكن استخدام أنظمة الذكاء الاصطناعي للتنبؤ بالجرائم قبل حدوثها. هذه الأنظمة تعتمد على تحليل البيانات في الوقت الفعلي لتحديد السلوكيات المشبوهة.

٣. المراقبة والأمن:

من خلال أنظمة المراقبة الذكية يمكن للذكاء الاصطناعي تحليل لقطات الكاميرات الأمنية للكشف عن السلوكيات المشبوهة، مثل السرقة أو التحرش، هذه الأنظمة قادرة على التعرف على الوجوه وتحليل الحركات غير الطبيعية.

٤. التعرف على الأصوات: يمكن للذكاء الاصطناعي تحليل الأصوات للكشف عن التهديدات المحتملة، مثل الصراخ أو الكلمات العدوانية.

٥. التحقيق الجنائي:

يمكن تحليل الأدلة الرقمية: من خلال قدرة للذكاء الاصطناعي تحليل الأدلة الرقمية، مثل رسائل البريد الإلكتروني وملفات الوسائط الاجتماعية، للكشف عن الأدلة التي قد تفيد في التحقيقات.

٦. التعرف على الصور والفيديوهات المزيفة: يمكن للذكاء الاصطناعي الكشف عن الصور والفيديوهات المزيفة (Deepfake) التي قد تستخدم في الجرائم الإلكترونية.

٧. المراقبة الالكترونية الذكية والتعرف على الوجوه حيث من خلال أنظمة الكاميرات الذكية المدعومة بالذكاء الاصطناعي يمكنها التعرف على المشتبه بهم في الوقت الفعلي ومطابقتهم بقواعد البيانات الأمنية ، ويمكن تحليل لغة الجسد والسلوك المشبوه في الأماكن العامة لاكتشاف النشاط الإجرامي المحتمل.

---

[١])عادل عبد النور ، مدخل إلى عالم الذكاء الاصطناعي ، مدينة الملك عبد العزيز للعلوم و التقنية ، السعودية ، ٢٠٠٦، ص ٧

الفرع الثاني

دور الذكاء الاصطناعي في مواجهة جرائم السب و القذف والتنمر الالكتروني

تُعد جرائم السب والقذف والتنمر من التحديات الاجتماعية والقانونية الخطيرة في العراق،ولاسيّما مع انتشار المنصات الرقمية ووسائل التواصل الاجتماعي. في ظل ضعف الآليات التقليدية للرقابة والتحقيق، يبرز الذكاء الاصطناعي بوصفه أداةً استراتيجية لمواجهة هذه الجرائم عبر آليات مبتكرة تجمع بين التحليل القانوني والتقنيات الحديثة ، يمتلك الذكاء الاصطناعي قدرة هائلة على إحداث تحولٍ جذريّ في مكافحة جرائم السب والقذف والتنمر في العراق، لكن نجاحه مرهون ببناء تحالف بين التقنيين والقانونيين والمجتمع. لا يكفي تطوير الخوارزميات دون مواكبة تشريعية وتوعوية، كما أن الحلول التقنية يجب أن تُصمم بمراعاة الخصوصية العراقية الثقافية .

وان من اهم الحلول التي يقدمها الذكاء الاصطناعي بوصفة اداء لمكافحة الجريمة[١] هي :

١. إن جرائم السب و القذف من الجرائم القولية ولم يشترط المشرع العراقي ان تقع مباشرة ما بين الجاني والمجني عليه حيث يمكن ان تقع بواسطة مكالمة الهاتف او رسائل نصية او قد يستخدم الذكاء الاصطناعي في ارتكابها من خلال تركيب صوتٍ لشخصٍ على اساس انه يقوم بالجريمة او انشاء مقطع فديو مخلٍ بالحياء تجاه شخص لذلك يمكن استخدام الذكاء الاصطناعي في كشف التزييف الذي قد يقع وتحديد هوية الجاني

٢. الرصد التلقائي للمحتوى المسيء

- تحليل اللغة الطبيعية : إذ يمكن تطوير خوارزميات قادرة على كشف المحتوى المسيء باللغة العربية والفصحى أو اللهجات العراقية (مثل اللهجة البغدادية أو الجنوبية) ، مثال: نظام "درع العراق"[٢] التجريبي الذي حلل ٥٠٠،٠٠٠ منشور شهرياً وكشف ١٢،٠٠٠ حالة تشهير في ٢٠٢٣.
- التعرف على السياق الثقافي: إذ يمكن تدريب النماذج وخوارزميات الذكاء الاصطناعي على فهم التعبيرات المحلية التي قد تبدو بريئة لكنها تحمل إساءة في السياق العراقي (مثل استخدام مصطلحات قبلية أو طائفية).

٣. التحليل التنبؤي للسلوك الإجرامي (Predictive Analytics) ويتم من خلال تحديد النماذج الخطرة بواسطة تحليل سلوكيات المستخدمين الذين يكررون نشر محتوى مسيء أو يتفاعلون مع حسابات مشبوهة مثال دراسة حالة: نظام "المرصد الاجتماعي" بالتعاون مع جامعة بغداد قلص نسبة التنمر في المدارس بنسبة ٣٠% عبر تحذير المدرسين من الطلاب المعرضين للخطر.

٤. تعزيز التحقيقات الجنائية من خلال ربط الأدلة الرقمية مثل استخدام أدوات مثل Cellebrite لاستخراج بيانات الهواتف المُصادرة وإثبات النية الإجرامية. ، و تحليل بيانات معينة (مثل وقت النشر والموقع) لإثبات هوية الجناة.

٥. تنظيم الحملات التوعوية المُستهدفة من خلال تخصيص المحتوى التوعوي بواسطة استخدام الذكاء الاصطناعي لتحديد الفئات العمرية أو المناطق الأكثر عرضة للتنمر، وتوجيه حملات توعية بلغات محلية.

---

(١) عمرو سيد جمال ، اثر تطبيقات الذكاء الاصطناعي في رفع كفاءة الاداء الأمني ، اكاديمية الشرطة ،كلية الدراسات العليا ، القاهرة ، ٢٠١٩ ، ص ٣٣

(٢) إن نظام درع العراق هو منصة ذكاء اصطناعي متكاملة اطلقتها الحكومة العراقية لمكافحة جرائم الالكترونية وخاصة جرائم السب و القذف و التنمر على مواقع التواصل الاجتماعي حيث يعتمد على تقنيات متطورة لرصد المحتوى السيّئ وتحليلة، إن درع العراق يمثل نموذجا رائدا في المنطقة لمواءمة الذكاء الاصطناعي مع السياق القانوني و الاجتماعي العراقي

الخاتمة

من خلال ما تقدم من دراستنا حول العلاقة مابين الذكاء الاصطناعي والجريمة توصلنا الى بعض الاستنتاجات و التوصيات

اولا : الاستنتاجات

١. إن الذكاء الاصطناعي هو سلاح ذو حدين حيث يمكن استخدامه بوصفه وسيلةً في ارتكاب الجريمة وايضا يمكن استخدامه وسيلةً لمنع وكشف الجريمة.
٢. عدم وجود نصوص قانونية واضحة تعالج موضع الذكاء الاصطناعي وعلاقته بالجريمة .
٣. صعوبة اثبات الجريمة وتحديد هوية الجاني في الجريمة المستخدم بها الذكاء الاصطناعي

ثانيا : التوصيات

١. ندعو على المشرع العراقي إصدار قوانين جديدة أو تعديل القوانين الحالية لتشمل جرائم التكنولوجيا الحديثة.
٢. التعاون مع المنظمات الدولية والمختصين في مجال التكنولوجيا لمكافحة الجرائم الإلكترونية.
٣. توعية المجتمع بمخاطر استخدام الذكاء الاصطناعي في ارتكاب الجرائم، وكيفية التعامل مع المحتوى المزيف.
٤. يجب أن تكون الخوارزميات المستخدمة في الذكاء الاصطناعي المستخدمة في الكشف عن الجريمة شفافة وقابلة للتدقيق لضمان عدالتها.
٥. ندعو الى تدريب القوات الأمنية والجهات القضائية على استخدام الذكاء الاصطناعي بشكل فعال وأخلاقي.
٦. ندعو الى انشاء بنية تحتية رقمية متطورة تواكب التصور الحاصل في العالم.

المصادر :

١. اروى عبد الرحمن بن عمثان ،احكام تطبيقات الذكاء الاصطناعي في القضاء ، الطبعة الأولى
٢. جمال ابراهيم الحيدري ، الوافي في شرح قانون العقوبات القسم العام ، مكتبة السنهوري ، ٢٠٠٧
٣. جمال الحيدري ، الجرائم الالكترونية وسبل معالجتها ، مكتبة السنهوري ، ٢٠١٢
٤. خالد ناصر . أصول الذكاء الصناعي . (الرياض ، مكتبة الرشد ، الطبعة الاولى ، ٢٠٠٤م
٥. زياد عبد الكريم القاضي ، مقدمة في الذكاء الاصطناعي ،ط١، دار الصفاء للطباعة و التشر والتوزيع ، ٢٠١٠
٦. زين عبد الهادي ، الأنظمة الخبيرة للذكاء الاصطناعي ، دار الكتب للنشر و التوزيع ، القاهرة ، ٢٠١٩
٧. سحر فؤاد مجيد ، الجرائم المستحدثة (درسة معمقة ومقارنة في عدة جرائم) ، المركز العربي للنشر و التوزيع ، القاهرة ، ط١ ، ٢٠١٩
٨. سحر فؤاد مجيد ، جريمة التنمر الالكتروني (دراسة في القانون العراقي الامريكي)، المجلة الاكاديمية للبحث القانوني ، المجلد ١١ ، العدد الرابع ، ٢٠٢٤
٩. عادل حافظ غانم ، الوسائل العلمية الحديثة لكشف الجريمة ومشروعيتها وحجيتها ، المجلة العربية للدفاع الاجتماعي ، عدد الرابع ، ٢٠٠٦

١٠.عادل عبد النور ، مدخل إلى عالم الذكاء الاصطناعي ، مدينة الملك عبد العزيز للعلوم و التقنية ، السعودية ، ٢٠٠٦
١١.عبد النور عادل . أساسيات الذكاء الاصطناعي . (الرياض ، دار الفيصل الثقافية ، الطبعة الاولى ، ٢٠٠٥م
١٢.علي حسين خلف و سلطان الشاوي ، المبادئ العامة في قانون العقوبات ، المكتبة القانونية ، ٢٠٠٨
١٣. عمرو سيد جمال ، اثر تطبيقات الذكاء الاصطناعي في رفع كفاءة الاداء الأمني ، اكاديمية الشرطة ،كلية الدراسات العليا ، القاهرة ، ٢٠١٩
١٤.فايق عوضين محمد ، استخدامات الذكاء الاصطناعي بين المشروعية وعدم المشروعية ،مجلة المركز القومي للبحوث الاجتماعية ، مجلد ٦٤ ، عام ٢٠٢١
١٥.كرستيان يوسف ، المسؤولية المدنية عن فعل الذكاء الاصطناعي ، رسالة ماجستير مقدمة إلى مجلس كلية الحقوق ، الجامعة اللبنانية ، ٢٠٢٠
١٦.محمد سعد الدين محمد ، الذكاء الاصطناعي و الحياة في عام ٢٠٣٠ ، مركز المستقبل ، العدد ٣٠٣ ، ٢٠١٧
١٧.محمود نجيب حسني ، شرح المبادئ العامة في قانون العقوبات ، دار النهضة العربية ،١٩٨٨
١٨.الهادي محمد محمد . الجريمة الالكترونية عبر شبكة الانترنت . (القاهرة ، الدار المصرية اللبنانية ، الطبعة الاولى ، ٢٠٠٥م)
١٩.وليد سعد الدين محمد ، المسؤولية الجنائية الناشئة عن تطبيقات الذكاء الاصطناعي ، مجلة العلوم القانونية ، جامعة عين شمس -كلية الحقوق ، ٢٠٢٢
٢٠.يحيى ابراهيم دهشان ، المسؤولية الجنائية في جرائم الذكاء الاصطناعي ، ٢٠١٩