استخدام الذكاء الاصطناعي في مكافحة الجرائم السيبرانية

د. احمد عبد السلام السعدون
جامعة النهرين / قسم الشؤون الإدارية والمالية
Ahmedalsadoun9@gmil.com

م. د سلمى غضبان حسين

كلية الادارة والاقتصاد/ الجامعة المستنصرية

Salma_law@uomustansiriyah.edu.iq

ملخص البحث:

تتزايد جرائم الانترنيت في الوقت الحالي بشكل سريع وملحوظ وذلك بسبب ان التكنلوجيا تنمو بسرعة كبيرة وفائقة، لذا فأن التحقيق في الجرائم السيبرانية واثباتها اصبح امرا مهماً جدا.

فالأنترنيت اليوم هو اسرع بنية أساسية في حياة كل انسان فهو قادر على ارسال واستقبال أي شكل من اشكال البيانات، لذلك اصبح المجرمون يستخدمون الفضاء الالكتروني، لارتكاب العديد من الجرائم السيبرانية اذ تتعرض البنية السيبرانية لدرجة كبيرة من التطفل والتهديد خاصة مع عدم قدرة أجهزة الحماية على حماية الفضاء الالكتروني، كما ان الجريمة السيبرانية لم تعد تقتصر على النطاق المحلي بل هي تهديد عالمي لأي نظام كومبيوتر في العالم ولذلك نحتاج الى أساليب مبتكرة مثل تطبيق الذكاء الاصطناعي الذي يوفر المرونة والقدرة على التعلم للبرامج والتي من شأنها مساعدة المختصين في التحقيق واثبات الجرائم السيبرانية، من خلال الوقوف على التقدم الذي تحقق في مجال الذكاء الاصطناعي لمكافحة الجريمة السبرانية، من خلال متابعة التطورات الحاصلة في تلك التطبيقات والتي من خلالها يمكن القضاء على التهديدات التي تلحق الفضاء الالكتروني.

الكلمات المفتاحية : الذكاء الاصطناعي، الجريمة ، الجرائم السيبرانية ، مكافحة الجريمة

Using artificial intelligence to combat cybercrime

dr. Ahmed Abdel Salam Hassan

University of Nahrain / Department of Administrative and Financial Affairs

Assist.Dr. Salma Ghadban Hussein

College of Administration and Economics / Al-Mustansiriyah University

Abstract

Internet crimes are currently increasing rapidly and significantly because technology is growing very quickly, so investigating and proving cybercrimes has become a very important matter.

The Internet today is the fastest infrastructure in every human being's life, as it is capable of sending and receiving any form of data. Therefore, criminals have begun to use cyberspace to commit many cybercrimes, as the cyberstructure is exposed to a large degree of intrusion and threat, especially with the inability of security devices to protect... Cyberspace.

Also, cybercrime is no longer limited to the local scope, but rather is a global threat to any computer system in the world. Therefore, we need innovative methods such as applying artificial intelligence, which provides flexibility and the ability to learn for programs that will help specialists investigate and prove cybercrimes, By examining the progress achieved in the field of artificial intelligence to combat cybercrime, by following up on developments in these applications, through which threats to cyberspace can be eliminated.

Keywords: Artificial intelligence, crime, cybercrime, crime control.

المقدمة

بات الذكاء الاصطناعي محل اهتمام الدول في شتى المجالات ومنها المجال القضائي في مكافحة الجرائم السيبرانية ومدى إمكانية الاستعانة بهذه التقنيات في هذا المجال، وذلك بهدف حماية المجتمع من هذه الجرائم وتبعاتها وبالتالي استخدام كافة الوسائل الممكنة والمتاحة للحد من وقوع الجريمة ومكافحتها.

ولقد اصبح الذكاء الاصطناعي يغزو كافة المؤسسات الرسمية وغير الرسمية وكذلك منازل المواطنين في المجتمع، فالذكاء الاصطناعي يشمل اية آلة او جهاز يحتوي على أجزاء الكترونية من خلال التحكم بهذه الآلة او الجهاز عن بعد ولكن بأيادي بشرية بما يتضمن ذلك توقيتات مبرمجة بشكل مسبق.

على الرغم مما يجلبه الذكاء الاصطناع من رفاهية وتطور بحيث يسهل الحياة البشرية، الا انه قد يساء استخدامه وذلك من خلال إمكانية استخدام هذه الأجهزة الالكترونية في ارتكاب الجرائم مما يسبب اذى كبير للمجتمع.

فلقد ظهر هذا الذكاء الاصطناعي بصوره وتقنياته المتعددة في الآونة الأخير بشكل كبير، حتى بات جزءاً لا يتجزأ من حياة البشر، فأتسعت مجالات عمله واستخداماته في الأعمال العسكرية بادئ الأمر الى شتى مجالات الحياة كالصحة والصناعة والتجارة والتعليم والإدارة.

واصبح الهاتف وأجهزة الكمبيوتر في كل بيت وبيد كل شخص والتي تعد من أهم تقنيات الذكاء الاصطناعي التي تحاكي العقل البشري من خلال استقبال البيانات وتحليلها لتقوم بمهام الانسان بدلاً منه ومن امثلتها الروبوتات، وتتميز الجرائم السيبرانية بكونها عابرة للحدود تحدث في مكان معين ويكون ضحاياها في مكان آخر، بالإضافة الى سرعة تنفيذها وكذلك سرعة اتلاف الأدلة ومحو آثارها، فضلاً عن كونها ترتكب من أشخاص يتمتعون بذكاء عالي.

اهداف البحث:

يهدف البحث الى بيان مدى إمكانية استخدام وسائل الذكاء الاصطناعي في مكافحة هذا النوع من الجرائم المتطورة وبالتالي تحقيق اقصى استفادة ممكنة من استخدام هذا الذكاء لا في مجال ارتكاب الجرائم بل في مكافحتها.

مشكلة البحث:

تكمن مشكلة البحث في طبيعة تقنية الذكاء الاصطناعي التي ما زالت في طور الاستكشاف من حيث طبيعة العمل ومجالات الاستخدام فالمشكلة الرئيسية للبحث حول إمكانية استخدام هذه التقنيات في مكافحة الجرائم السيبرانية؟ والتي تدفعنا الى عدة تساؤلات على النحو الآتي:

1- ماهو مفهوم الذكاء الاصطناعي واساليبه؟

2- ماهي أنواع الجرائم السيبرانية؟

3- ما هو دور تقنيات الذكاء الاصطناعي في الوقاية من الجريمة والحد منها.

منهج البحث:

اعتمد الباحث في هذه الدراسة على المنهج التحليلي القائم على تحليل النصوص القانونية وكذلك المنهج المقارن من خلال بيان اراء الفقهاء في كل من مصر وفرنسا والعراق.

خطة البحث:

تم تقسيم هذا البحث الى مبحثين حيث سندرس في المبحث التعريف بالذكاء الاصطناعي والجريمة السيبرانية، في حيث سنبحث في المبحث الثاني عن دور الذكاء الاصطناعي في مكافحة الجريمة.

المبحث الأول : التعريف بالذكاء الاصطناعي والجريمة السيبرانية

يعد الذكاء الاصطناعي من تقنيات التكنولوجيا الحديثة ولا تكاد تخلو مؤسسة او بيت من أجهزة الذكاء الاصطناعي، وأصبحت جزءاً من حياة البشر، ولا يمكن الاستغناء عن هذه الأجهزة فهي موجودة في الهواتف الشخصية وفي الحواسيب وفي السيارات وفي أنظمة المؤسسات الرقابية والأمنية مثل كاميرات المراقبة وأجهزة الإنذار والتسجيل وفي الأنظمة الوقائية كأنظمة إطفاء الحريق وغيرها[1].

لما تقدم سنقوم بتقسيم هذا المبحث على مطلبين حيث سنخصص المطلب الأول لبيان مفهوم الذكاء الاصطناعي في حيث سندرس في المطلب الثاني مفهوم الجريمة السيبرانية.

المطلب الأول : مفهوم الذكاء الاصطناعي

مع تطور الحاسبات الآلية في الحقبة الأخيرة واتضاح بعض معالم مكونات الدماغ البشري، اصبح لدى الكثير من الباحثين الرغبة الملحة في استعارة مكونات الدماغ البشري ومحاولة برمجتها في الحاسوب، وقد كان ذلك مدخلاً لانتشار علم الذكاء الاصطناعي وتطبيقات المختلفة وبالرغم من

1 - د. عماد الدحيات ، نحو تنظيم قانوني للذكاء الاصطناعي في حياتنا، بحث منشور في مجلة الاجتهاد للدراسات القانونية والاقتصادية، كلية القانون، جامعة الامارات العربية المتحدة، المجلد 8، ع5 ، 2019 ، ص16.

المميزات العديدة لها الا انها في الوقت نفسه تمثل الكثير من التداعيات السلبية، إذ تجعل حياة الأفراد اكثر عرضة للهجمات الالكترونية كما انها تجعل معلومات الدولة وبنيتها التكنولوجية عرضة للهجمات الالكترونية.

للذكاء الاصطناعي تعريفات عديدة تختلف فيما بينها من حيث الألفاظ والتراكيب، في الوقت الذي يتشابه مضمونها الى حد بعيد، ومن تلك التعريفات : (الأنظمة والأجهزة التي تحاكي الذكاء البشري لأداء المهام والتي يمكنها ان تحسن من نفسها استناداً الى المعلومات التي تجمعها)[1].

وقد عرفه (جوني ماكارثي) بأنه: (علم وهندسة صناعة الآلات الذكية وخاصة برامج الكمبيوتر الذكية، او هو فرع من علوم الكمبيوتر الذي يهدف الى انشاء الآلات الذكية)[2].

ويعرف الذكاء الاصطناعي بأنه : (سلوك وخصائص معينة تتسم بها برامج الحاسبات الآلية التي تجعلها تحاكي القدرات الذهنية البشرية وأنماط عملها ومن أهم تلك الخواص : القدرة على التعلم والأستنتاج ورد الفعل الإيجابي السريع، فالذكاء الاصطناعي هو قدرة الآلة على محاكاة العقل البشري وطريقة عمله مثل القدرة على التفكير والاكتشاف والاستفادة من التجارب السابقة)[3].

وقد عرفت اللجنة الاستشارية الوطنية للأخلاقيات بفرنسا الذكاء الاصطناعي بانه: (تركيبة برامج معلوماتية مكرسة للقيام بمهام ينجزها الإنسان بشكل اكثر إرضاء[4].

مما تقدم يتضح لنا من التعريفات السابقة للذكاء الاصطناعي بانها عبارة عن جعل الحاسوب او اية آلة تعمل بالبرمجة أداة تساعد في استخلاص النتائج.

و يمكننا تعريف الذكاء الاصطناعي بأنه : مجموعة معلومات قائمة على الأنظمة والتقنيات والتي يتم برمجتها ضمن الأجهزة والآلات التي تحاكي الذكاء البشري في التعامل مع الاحداث وبالتالي إيجاد الحلول لها.

تجدر الإشارة الى ان تقنيات الذكاء الاصطناعي قد مرت بتطورات كبيرة بمرور الزمن والتراكم المعرفي والتقني، واستقرت في نهاية المطاف على عدد من الصور في طائفة واسعة المجالات منها:

1- **الذكاء الاصطناعي الكلاسيكي:** وهذا النوع قائم على قواعد الشرط المنطقي وكان يتطلب المزيد من العمل البشري من خلال ادخال روابط وفواصل في التعليمات التي تشغل بها الأجهزة الالكترونية[5].

1 - د. عبد الله موسى ، د. احمد حبيب بلال، الذكاء الاصطناعي ثورة في تقنيات العصر، القاهرة ، المجموعة العربية للتدريب والنشر، 2019 ، ص20.
2 - د. منال البلقاسي ، الذكاء الاصطناعي صناعة المستقبل ، دار التعليم الجامعي ، الإسكندرية ، 2019 ، ص13.
3 - د. محمود مختار ، تطبيقات الذكاء الاصطناعي، بحث منشور في المجلة الدولية في العلوم التربوية ، المؤسسة الدولية لآفاق المستقبل ، مجلد3، ع4، 2020، ص183.
4 - نقلاً عن د. عمار ياسر زهير البابلي ، الآليات الحديثة لحماية وتأمين نظم المعلومات وآثارها على المنظومة الأمنية ، رسالة دكتوراه ، كلية الدراسات العليا ، اكادمية الشرطة ، القاهرة، 2018، ص45.
5 - الآن بونية : الذكاء الاصطناعي ،ترجمة د. صبري فرغلي ، سلسلة عالم المعرفة ، المجلس الوطني للثقافة والفنون والآداب ، الكويت ، 1993 ، ص13.

2- **الأنظمة الخبيرة:** وهي قائمة على قواعد ونماذج مستخلصة من مجموعات كبير من الخبرات والمعلومات التي يتم تغذية الحاسوب بها ومع التفاعل المعلوماتي بين القواعد، أصبحت هذه الأنظمة صعبة التطوير والتعديل.

3- **التعليم الآلي:** ويقوم هذا النوع من التقنيات على التحليل الدقيق لكميات كبيرة من البيانات، وبناء نماذج يمكن تعميمها اذا تطابقت المادة المبحوثة مع ما سبق تغذية الحاسوب بها، وهناك ثلاثة أنواع من التعليم الآلي تصنف حسب نسبة التدخل البشري وهي (خاضعة للإشراف البشري ، غير خاضعة للإشراف البشري، معززة للإشراف البشرية) وفي جميع الأحوال تحتاج هذه التقنية الى التدخل البشري للتعديل والتطوير[1].

4- **الشبكات العصبية الاصطناعية:** وتتكون من ثلاثة أنواع من الطبقات المترابطة من الخلايا العصبية الاصطناعية (طبقة ادخال ، طبقة حسابية وسيطة مخفية واحدة او اكثر، طبقة اخراج تقدم النتيجة).

5- **التعلم العميق:** يشير التعلم العميق الى الشبكات العصبية الاصطناعية التي تتكون من طبقات وسيطة متعددة، وهذا النهج هو الذي أدى الى العديد من التطبيقات الرائعة الحديثة للذكاء الاصطناعي مثل : معالجة اللغة الطبيعية، التعرف على الكلام، رؤية الحاسوب، انشاء الصور وغيرها[2].

خصائص الذكاء الاصطناعي

يتمتع الذكاء الاصطناعي بالعديد من الخصائص والمميزات نوجها بالآتي:[3]

اولاً: التمثيل الرمزي: حيث يتعامل الذكاء الاصطناعي مع رموز تعبر عن المعلومات المتوفرة وهو تمثيل يقترب من شكل تمثيل الانسان لمعلوماته في حياته اليومية.

ثانياً: البحث التجريبي: تتوجه برامج الذكاء الاصطناعي نحو مشكلات لا تتوافر لها حلول يمكن ايجادها تبعاً لخطوات منطقية محددة، إذ يتبع فيها أسلوب البحث التجريبي كما هو الحال فيمن يقوم بتشخيص مرض، إذ ان حساب الخطوة التالية يتم بعد بث احتمالات وافتراضات متعددة وهذا البحث التجريبي يحتاج الى ضرورة توافر سعة تخزين كبيرة في الكمبيوتر، كما تعتبر سرعة الكمبيوتر من العوامل المهمة لفرض الاحتمالات الكثير ودراستها[4].

ثالثا: احتضان المعرفة وتمثيلها: يجب ان تمتلك برامج الذكاء الاصطناعي في بنائها قاعدة كبيرة من المعرفة تحتوي على الربط بين الحالات والنتائج، فمثلاً اذا كان مشغل الأقراص في جهاز الكمبيوتر لا يقرأ البيانات المسجلة على القرص الجيد والكابل بين مشغل القرص فإن العطل يكون في مشغل الأقراص نفسه.

رابعاً: البيانات غير المكتملة: يجب على برامج الذكاء الاصطناعي أن تتمكن من إعطاء الحلول اذا كانت البيانات غير مؤكدة، وليس المعنى هنا ان تقوم باعطاء الحلول مهما كانت الحلول خاطئة

1 - د. منال البلقاسي ، الذكاء الاصطناعي صناعة المستقبل ، مصدر سابق، ص23.

2 - George F. Luger , Artificial Inteligence ; Structures and Strategies for Complex Problem Solving , Addison – Wesley , 2002 , p35.

3 - دعاء حاتم ، لمى العزاوي، الذكاء الاصطناعي والمسؤولية الجنائية الدولية بحث منشور في مجلة المفكر ، كلية الحقوق والعلوم السياسية ، جامعة محمد بسكرة ، الجزائر، ع 18 ، 2006 ، ص26.

4 - د. محمود مختار ، تطبيقات الذكاء الاصطناعي ، مصدر سابق، ص82.

ام صحيحة، بل يجب لكي يقوم الذكاء الاصطناعي بأدائه الجيد ان يكون قادراً على إعطاء الحلول المقبولة والا يصبح مقصراً[1].

خامساً: القدرة على التعلم: تعد القدرة على التعلم هي احدى مميزات السلوك الذكي، وسواء كان التعلم يتم عن طريق الملاحظة او الاستفادة من أخطاء الماضي فأن برامج الذكاء الاصطناعي يجب ان تعتمد استراتيجيات لتعليم الآلة[2].

اما عن مميزات الذكاء الاصطناعي فهو يتمتع بالعديد من المميزات أهمها :[3]

1- استخدام تقنيات الذكاء الاصطناعي في حل المشكلات المعروضة في ظل غياب المعلومة الكاملة عنها.

2- التفكير والادراك.

3- اكتساب المعرفة وتطبيقها.

4- التعلم والفهم من التجارب والخبرات السابقة.

5- الاستجابة السريعة للمواقف والظروف الجيدة.

6- التعامل مع الحالات الصعبة والمعقدة.

المطلب الثاني : مفهوم الجريمة السيبرانية

لم يعرف المشرع العراقي، شأنه شأن جل التشريعات المقارنة الجريمة السيبرانية، والسبب في ذلك يرجع الى أن وضع التعريفات للمفاهيم القانونية العامة هو عمل فقهي وليس من عمل المشرع. لذلك يعرف الفقه القانوني الجريمة بصفة عامة على انها: (فعل غير مشروع صادر عن إرادة جرمية يقرر له القانون العقوبة أو التدبير احترازياً)[4].

كما يعرف الفقه القانوني الجريمة بصفة عامة: (كل تصرف جرمه القانون سواء كان إيجابيا أو سلبيا كالامتناع ما لم ينص على خلاف ذلك)[5].

أما بالنسبة لمفهوم الجريمة السيبرانية فلم يتفق الفقهاء والباحثون على التعريف موحد لهذه الأخيرة، فمنهم من ينظر إلى موضوع الجريمة في حد ذاتها، وهناك من ينظر إلى الوسيلة المستعملة في ارتكابها، غير أنهم لم يتفقوا على تسمية موحدة لهذا النوع الجديد من الجرائم التي تباينت تسمياتها عبر مراحل زمنية ارتبطت بتقنية المعلومات، فهناك من يطلق عليها بتسمية الجرائم السيبرانية

1 - د. محمود مختار ، مصدر سابق، ص82.
2 - غادة المنجم: الذكاء الاصطناعي وعلاقته بنظم مساندة القرار، رسالة ماجستير ، كلية العلوم الإدارية، جامعة الملك سعود، الرياض، 2012، ص19.
3 - سارة أمجد عبد الهادي ، الذكاء الاصطناعي في ظل القانون الجزائي ، أطروحة دكتوراه ، كلية الدراسات العليا ، جامعة القدس ، فلسطين ، 2022، ص6.
4 - د. عباس الحسني، شرح قانون العقوبات العراقي الجديد، المكتبة القانونية ، بغداد، بدون سنة نشر، ص87.
5 - د. علي حسين الخلف ، د. سلطان عبد القادر الشاوي ، المبادئ العامة في قانون العقوبات ، العاتك لصناعة الكتاب ، القاهرة ، ط2 ، 2010 ص132

(cybre crime)، وهناك من يطلق عليها بتسمية إساءة استخدام تكنولوجيا المعلومات والاتصال، كما يطلق عليها أيضا بجرائم الكمبيوتر والأنترنيت[1].

وقد عرفها المشرع الإماراتي في مرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية حيث نصت على: (كل استهداف متعمد ومخطط للأنظمة المعلوماتية أو البنية التحتية أو الشبكات الإلكترونية أو وسائل تقنية المعلومات يقلل من قدرات ووظائف أي منها، سواء كان ذلك لغرض شخصي أو لأغراض الاعتراض أو التسلل أو الاختراق أو التسريب أو بغرض تعريض البيانات أو المعلومات للخطر أو تعطيل العمليات وما في حكمها)[2].

أولا: خصائص الجريمة السيبرانية

تتميز الجرائم السيبرانية بخصائص فريدة تجعلها مختلفة عن الجرائم التقليدية، تلك الفروقات تعود إلى سماتها الفريدة والعناصر التي تشكلها بالإضافة إلى الأدوات والوسائل التي تستخدم في تنفيذ الجرائم السيبرانية وتتمثل هذه الخصائص في :[3]

1- جرائم تتم عبر التقنيات التكنولوجية الحديثة، وعلى راسها شبكة الأنترنيت التي تعتبر كوسيلة لارتكابها.

2- تستهدف الجرائم السيبرانية الأنظمة المعلوماتية من خلال اختراقها بهدف تلاعب أو تشويه المعلومات والبيانات الخاصة بمستخدمي البيئة الرقمية، على غرار ما يحدث في الجرائم التقليدية.

3- تعتبر جريمة ناعمة بسبب خفتها، حيث قد لا يلاحظ الشخص المتضرر ارتكابها أثناء تواجده على الشبكة، فالجاني يمتلك مهارات تقنية متقدمة تسمح له بالقيام بتلك الجرائم دون أن يتم الكشف عنها، مثل سرقة الأموال أو إرسال فيروسات ضارة إلى البرامج وأجهزة الكمبيوتر[4].

4- تعتبر من الجرائم التي يصعب اكتشافها ولذلك لعدم تركها لآثار مادية يمكن من خلالها كشف مرتكبها هذه الأخيرة، مما يجعل الأمور تزداد تعقيداً لدى سلطات الأمن وأجهزة التحقيق، فداخل هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات إلكترونية غير مرئية، مما يجعل أمر طمس هذا الدليل الإلكتروني ومحوه كليا من قبل الفاعل أمر في غاية السهولة.

5- تعتبر من الجرائم العابرة للحدود حيث لا تعترف بعنصر الزمان والمكان، فهي تتميز بالتباعد الجغرافي واختلاف التواقيت بين الجاني والمجني عليه.

6- تعتبر من بين الجرائم التي يتطلب إلمام مرتكبها بجوانب التقنية وكذلك الخبرة الفائقة في استخدام الحاسب الآلي.

1 - محمود سعد عبد المجيد ، الجرائم السيبرانية وانعكاسات ثورة التكنولوجيا على النظرية العامة للجريمة ، دار المطبوعات الجامعية ، الإسكندرية ، 2023، ص33.
2 - ينظر : المادة (1) من المرسوم رقم (34) لسنة 2021 الاماراتي في شان مكافحة الشائعات والجرائم الالكترونية.
3 - بلال أمين زين الدين: جرائم نظم المعالجة الالية للبيانات ، دار الفكر الجامعي ، الاسكندرية، 2008، ص71.
4 - ممدوح عبد الحميد عبد المطلب ، جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية ، دار الفتح للطباعة والنشر، الامارات، 2000، ص26.

ثانياً: اركان الجريمة السيبرانية

يتطلب الكشف عن الجريمة السيبرانية توافر أركان محددة، المتفق على ضرورة توافرها على أرض الواقع في أية جريمة أخرى، بدون هذه الأركان، يصعب تأكيد وجود هذه الجريمة.

أن الجريمة السيبرانية لا تختلف عن الجرائم التقليدية التي ينص عليها قانون العقوبات، فهي تتطلب وجود عناصر محددة يجب توافرها في أي جريمة، وهذا يشمل الجرائم السيبرانية كجزء من القوانين الجنائية العامة، هذا النوع من الجرائم يتطلب وجود ركنين أساسيين: ركن مادي وركن معنوي:

1- الركن المادي للجريمة السيبرانية:

في إطار الجريمة محل البحث، يتعين أن يأتي الركن المادي للجريمة السيبرانية على الشكل والهيئة التي يتطلبها المشرع، سواء من حيث اجتماع عناصره الثلاثة من نشاط أو سلوك مادي وعلاقة سببية ونتيجة إجرامية، أو أن يكتفي المشرع بعنصر وحيد وهو النشاط أو السلوك المادي فقط، وفى هذه الحالة تتوافر الجريمة دون حاجة للبحث عن النتيجة المتحققة وعلاقة السببية، حتى وإن توافرت على المستوى المادي، فإن هذا الوجود يعد من طبيعة مادية ليس له في القانون من أثر (جريمة شكلية) أو كما يسميها بعض أصحاب الفقه الجنائي جريمة السلوك والنشاط فإن النشاط أو السلوك المادي يتمثل في الفعل الذي يأتيه الجاني بالمخالفة لإرادة المشرع ويتعين أن يكون له مظهر خارجي[1].

وهو يمثل عنصر جوهريًا لقيام الركن المادي في كافة أنواع الجرائم المادية والشكلية، والمراد بالسلوك النشاط الخارجي الذي يقوم به الجاني، ويبرز في العالم الخارجي مكونا لماديات الجريمة ومسببا لما قد يترتب عليها من ضرر أو خطر، وسواء قصد الجاني من هذا السلوك الإجرامي تحقيق نتيجة معينة أم تحققت النتيجة دون أن تنصرف إرادته إليها ويختلف النشاط أو السلوك المادي من جريمة لأخرى، كما يختلف في الجرائم السيبرانية عنه في الجرائم التقليدية، إذ يتطلب السلوك المادي في الجرائم السيبرانية وجود بيئة رقمية[2]، كما يتطلب السلوك المادي في الجرائم السيبرانية أيضا معرفة بداية هذا النشاط والشروع فيه ونتيجته، فمثلا يقوم مرتكب الجريمة بتجهيز الحاسب لكي يحقق له حدوث الجريمة ، فيقوم بتحميل برنامج اختراق أو أن يقوم بإعداد هذا البرنامج بنفسه، وآنذاك قد يحتاج إلى تهيئة صفحات تحمل في طياتها مواد خليعة أو مخلة بالآداب العامة وتحميلها على الجهاز المضيف (Hosting Server) ، كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيدا لبثها[3].

ولكن ليست كل جريمة تستلزم وجود أعمال تحضيرية، فالسلوك الإجرامي في الجريمة السيبرانية يرتبط دائما بالمعلومة المخزنة على الحاسب الآلي وتكمن صعوبة المشكلة في أن السلوك الإجرامي

1 - محمود سعد عبد المجيد ، الجرائم السيبرانية وانعكاسات ثورة التكنولوجيا على النظرية العامة للجريمة ، دار المطبوعات الجامعية ، الإسكندرية ، 2023، ص47.

2 - المقصود بالبيئة الرقمية: هو مجموعة المواد نصوص أو صور اوفيديوهات وغيرها مخزنة بصيغة رقمية ويمكن الوصول إليها عبر عدة وسائط وأهم وسائل الوصول لمحتوى الرقمية على الكتب الرقمية فقط يتعداه إلى غيرها من الوسائط واتصال بالإنترنت من خلال الحاسب الآلي أو الهاتف الذكي. نقلاً عن محمود سعد عبد المجيد ، الجرائم السيبرانية وانعكاسات ثورة التكنولوجيا على النظرية العامة للجريمة، مصدر سابق ، ص47.

3 - هبة ممدوح إبراهيم ، الجوانب الإجرائية لجرائم الانترنيت، دار الفكر الجامعي ، الإسكندرية ، 2019، ص18.

قد يتحقق بمجرد ضغطة زر في لوحة المفاتيح الملحقة بالحاسب فيتم " مثلا " تدمير نظام أرصدة العملاء في أحد البنوك، أو إساءة استعمال بطاقات الائتمان.

وقد أصبح هذا السلوك محلا لتساؤلات عديدة خاصة فيما يتعلق ببدايته أو الشروع في ارتكاب الجريمة، فهو يختلف عما عليه الحال في العالم المادي. فقد عد المشرع الفرنسي الشروع كالجريمة التامة في نطاق الجرائم السيبرانية، إذ عد جريمة الدخول غير المشروع أو البقاء غدرا بالأنظمة الآلية لمعالجة المعلومات المنصوص عليها في المادة (323 \ 1) من قانون العقوبات الفرنسي لسنة 1994 المعدل جريمة بحد ذاتها، حيث نصت هذه المادة على أن: (كل شخص قام بالدخول أو البقاء بطريقة كلية أو جزئية داخل نظام لمعالجة المعلومات سيعاقب بالحبس الذي لا يقل عن شهرين ولا يزيد عن سنة وبغرامة تتراوح بين 30000 إلى 50000 فرنك أو بإحدى هاتين العقوبتين كل من دخل بطريق الغش أو مكث غدرا في نظام للمعالجة الآلية للمعلومات أو في جزء منه...).

2- الركن المعنوي للجريمة السيبرانية:

الركن المعنوي هو الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، وبالنظر لما للركن المعنوي من أهمية أساسية في النظرية العامة للجريمة، إذ الأصل أنه لا جريمة بدون ركن معنوي، فهذا الركن هو سبيل المشرع إلى تحديد المسؤولية عن الجريمة، فإنه يتعين توافر الركن المعنوي في الجريمة السيبرانية بالرغم من أنها لا ترتكب في عالم مادي وإنما في عالم افتراضي، فيجب أن يكون الجاني عالما بأن الفعل الذي يأتيه أو سلوكه المادي يجرمه القانون، وعلى الرغم من توافر هذا العلم لديه تتجه إرادته إلى إتيان هذا الفعل قاصدا تحقيق نتيجته[1].

وقوام الركن المعنوي، هو الأصول النفسية لماديات الجريمة والسيطرة النفسية عليها، ومن ثم كان الركن المعنوي في جوهره قوة نفسية، وهذه القوة هي الإرادة، إلا أن هذا الركن لا يتحقق بهذه الإرادة وحدها ما لم تتجه إلى إتيان فعل جرمه القانون فالإرادة هي جوهر الركن المعنوي، كما أنها دليل على خطورة شخصية الجاني، وهي مظهر لهذه الشخصية فإذا اتخذت هذه الإرادة صورة القصد الجنائي وصفت الجريمة بأنها عمدية، أما إذا اتخذت صورة القصد غير العمدي فإن الجريمة توصف بأنها غير عمدية[2].

ويعتمد هذا التقسيم على أن الفاعل في الجريمة العمدية قد قام باقتراف فعله قاصدا ارتكاب السلوك المجرم الذي أتاه، كما أراد النتيجة الإجرامية التي حصلت منه أو أية نتيجة أخرى، بينما أن الفاعل في الجريمة غير العمدية لم يقصد سوى ارتكاب السلوك دون إرادة تحقيق النتيجة الإجرامية.

المبحث الثاني : دور الذكاء الاصطناعي في مكافحة الجرائم السيبرانية

لقد تزايدت الجرائم السيبرانية في الآونة الحديثة بشكل سريع جداً بسبب النمو السريع للتكنولوجيا، لذلك فأن التحقيق في الجرائم السيبرانية ومكافحتها اصبح في غاية الأهمية، بالإضافة الى كونه مهمة معقدة في حال قيامها، فهناك الكثير من الجرائم الالكترونية في وقتنا الحالي وفي المستقبل، فالانترنيت هو اسرع بنية أساسية في حياة كل انسان، فهو قادر على ارسال واستقبال أي شكل من

1 - محمود سعد عبد المجيد ، الجرائم السيبرانية وانعكاسات ثورة التكنولوجيا على النظرية العامة للجريمة، مصدر سابق ، ص51.

2 - هبة ممدوح إبراهيم ، الجوانب الإجرائية لجرائم الانترنيت، مصدر سابق ، ص23.

أشكال البيانات، ولا يقتصر الامن السيبراني على تأمين تكنولوجيا المعلومات الخاصة بالصناعة بل يمتد الى تأمين الفضاء الالكتروني، ومع تقدم التكنولوجيا اصبح المجرمون يستخدمون الفضاء الالكتروني لارتكاب العديد من الجرائم السيبرانية.[1]

لما تقدم سنقوم بتقسيم هذا المبحث على مطلبين، حيث سندرس في المطلب الأول أنواع الجرائم السيبرانية، في حيث سنخصص المطلب الثاني لبيان الوسائل المستخدمة في مكافحة الجرائم السيبرانية وكالاتي:

المطلب الاول

أنواع الجرائم السيبرانية

الجريمة السيبرانية كما تم تعريفها في المبحث الأول هي اعمال غير قانونية يتم ارتكابها باستخدام الكمبيوتر، ويمكن ان يتم من خلال الجريمة السيبرانية ارتكاب اعمال السرقة والاحتيال والتزوير والتشهير والحاق الأذى، وعليه سنقوم بتوضيح أنواع الجرائم السيبرانية وفقاً للبيان الآتي:

اولا: جريمة الاعتداء على الشبكات والأنظمة

تنوعت جرائم الاعتداء على الشبكات والأنظمة بشكل كبير ولا يمكن حصرها، فمثل هذا النوع من الجرائم السيبرانية يكون متطور وينمو سريعاً، بالتالي لا يمكن تحديد أنواع محددة من هذه الجرائم والنص عليها في القوانين الخاصة، بل يكون تحديد مثل هكذا جرائم على سبيل المثال لا على سبيل الحصر، ومن أنواع هذه الجرائم نذكر ما يلي:

1- **جريمة الاختراق:** ان الدخول غير المشروع هو الوصول الى الموارد الوظيفية لجهاز الكمبيوتر او نظامه او شبكته وصولاً بدون أذن من المالك الشرعي او الشخص المسؤول، وقد نص قانون مكافحة جرائم تقنية المعلومات المصري على هذا النوع من الجرائم السيبرانية وعاقب عليه بمدة لا تقل عن سنة وبغرامة لا تقل عن 50 الفاً ولا تتجاوز 100 ألف جنيه، او احدى هاتين العقوبتين.[2]

وقد نص المشرع العراقي على هذه الجريمة وحدد لها عقوبة الحبس مدة لاتزيد على ثلاثة اشهر او بغرامة لاتقل عن مليوني دينار ولا تزيد عن خمسة ملايين دينار، وذلك في المادة (14/ ثالثا) من مشروع قانون جرائم المعلوماتية لسنة 2011، الا ان هذا القانون لم يرى النور الى حد هذه اللحظة.

2- **جريمة القرصنة والتخريب:** القرصنة هي كل فعل يرتكب بهدف اقتحام جهاز كمبيوتر او شبكة ويكون الدافع هو الرغبة في التدمير وتحقيق المكاسب الشخصية.[3]

1 - D.Dasgupta, Computational Intelligence in Cyber Security , IEEE International Conference on Computational for Homeland Security and Personal Safety , 2006 , p2-

2 - نصت المادة (14) من قانون مكافحة جرائم تقنية المعلومات المصري على انه : (يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن 50 الفا ولا تزيد عن 100 الف جنيه، او احدى هاتين العقوبتين كل من دخل عمداً او دخل بخطأ غير عمدي وبقي بدون و جه حق على موقع او حساب خاص او نظام معلوماتي محظور الدخول، فإذا نتج عن ذلك اتلاف او محو او تغيير او نسخ او أعاد نشر للبيانات او المعلومات الموجودة على ذلك الموقع او الحساب الخاص او النظام المعلوماتي تكون العقوبة الحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن 100 الف جنيه ولا تتجاوز 200 الف جنيه او بإحدى هاتين العقوبتين).

3 - هبة ممدوح إبراهيم ، الجوانب الإجرائية لجرائم الانترنيت، مصدر سابق ، ص37.

وقد نص قانون مكافحة جرائم تقنية المعلومات المصري في المادة (17) منه على انه: (يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن 100 الف جنيه ولا تتجاوز 500 الف جنيه، او بإحدى هاتين العقوبتين كل من اتلف او عطل او عدل مسار او الغى كلياً او جزئياً متعمداً وبدون وجه حق البرامج والبيانات او المعلومات المخزنة او المعالجة او المولدة او المخلقة على أي نظام معلوماتي وما في حكمة اياً كانت الوسيلة التي استخدمت في الجريمة).

3- جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة

تتمثل هذه الجريمة في الدخول العمدي وبدون وجه حق او من خلال تجاوز الحد المسموح به من حيث الزمان او من خلال اختراق موقع او بريد الكتروني او حساب خاص او نظام معلوماتي يدار بمعرفة او لحساب الدولة او احد الأشخاص الاعتبارية العامة، وقد عاقب المشرع المصري في المادة (20) من قانون مكافحة جرائم تقنية المعلومات بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن 50 الف جنيه ولا تتجاوز 200 الف جنيه.

ويشترط لتطبيق هذه المادة توافر الشروط الاتية:[1]

أ. ان يكون الجاني قد دخل بصورة عمدية او خطأ غير عمدي موقعاً او بريداً او حساباً خاصاً او نظاماً معلوماتياً.

ب. ان يدخل موقعاً او حساباً خاصاً او نظام معلومات، يدار بمعرفة او لحساب الدولة او لأحد الأشخاص الاعتبارية العامة.

ج. ان يتحقق علم الجاني بأن الموقع او الحساب الخاص او النظام المعلوماتي الذي دخل اليه يدار بمعرفة او لحساب الدولة او احد الأشخاص الاعتبارية.

4- الانتفاع بدون وجه حق من خدمات الاتصالات والمعلومات وتقنياتها:

ان سرقة ساعات الانترنيت تعني الاستخدام غير المصرح به لساعات الانترنيت التي يدفعها شخص اخر، ويعاقب قانون مكافحة جرائم تقنية المعلومات في المادة (13) بالحبس مدة لا تقل عن 3 أشهر وبغرامة لا تقل عن 10 ألف جنيه ولا تتجاوز 50 الف جنيه او بأحدى هاتين العقوبتين كل من انتفع بغير وجه حق عن طريق شبكة النظام المعلوماتي او احدى وسائل تقنية المعلومات بخدمة من خدمات اتصالات او خدمات قنوات البث المسموع والمرئي.

اما المشرع العراقي فقد عاقب على هذه الجريمة في المادة (14) من مشروع قانون جرائم المعلوماتية بالحبس مدة لا تزيد على 3 أشهر او بغرامة لا تقل عن مليوني دينار ولا تزيد على خمسة ملايين دينار كل من : هـ انتفع بدون وجه بخدمات الاتصالات عن طريق شبكة المعلومات او احد أجهزة الحاسوب.

ثانيا: الجرائم المرتبكة بواسطة الأنظمة وتقنيات المعلومات

وهناك ثلاث أنواع من هذه الجرائم وهي جرائم الاحتيال و جرائم اصطناع المواقع والحسابات الخاصة وجرائم الاعتداء على حرمة الحياة الخاصة وكالاتي:

1 - د. محمود رجب ، شرح قانون مكافحة جرائم تقنية المعلومات في ضوء القانون المصري، 175 لسنة 2018 ، دار الفكر الجامعي ، الإسكندرية ، ص745.

1- **جرائم الاحتيال عبر الانترنيت:** بالرغم لما يتمتع به الانترنيت من ميزات عظيمة في الاعمال التجارية والسرعة في انجاز الاعمال، الا انه يعتبر أداة بيد المجرمين في سبيل الاحتيال على الافراد.

فقد يقوم المحتالون بانشاء مواقع ويب تبدو اصليه لكنها في الواقع مزيفة في سبيل قيام المستخدم بإدخال معلوماته الشخصية وبالتالي يتم استخدام هذه المعلومات الشخصية في الوصول الى الحسابات التجارية والمصرفية.

وقد يقوم المجرم بأرسال رسالة عبر البريد الالكتروني يبلغ فيه المستخدم ان قد فاز بجائزة معينة وللحصول على المال يجب على المستلم الرد وبعد الرد يتم طلب تفاصيل حساب مصرفي ليتمكن المستخدم من تلقي الجائزة.

وقد عاقب المشرع المصري على هذا النوع من الجرائم بالحبس مدة لا تقل عن ثلاثة أشهر والغرامة التي لا تقل عن 30 الف جنيه ولا تتجاوز 50 الف جنيه.[1]

اما المشرع العراقي فقد نص في المادة (20/أولا) من مشروع قانون جرائم المعلوماتية على انه (يعاقب بالحبس وبغرامة لا تقل عن مليوني دينا ولا تزيد على خمسة ملايين دينار كل من استخدم أجهزة الحاسوب وشبكة المعلومات في أحد الأفعال الاتية:

أ- استخدام بقصد الغش علامة تجارية مسجلة في العراق باسم الغير كعنوان لموقعه على شبكة المعلومات.

ب- استخدام بطاقة الكترونية كوسيلة للوفاء مع علمه بعدم وجود رصيد له، او استعمل البطاقة المالية العائد للغير بدون علم صاحبها.

2- **جريمة اصطناع المواقع والحسابات الخاصة**

لقد عاقب المشرع المصري في المادة (24) من قانون مكافحة جرائم تقنية المعلومات على مثل هذا النوع من الجرائم بالحبس مدة لاتقل عن 3 أشهر وغرامة لا تقل عن 10 الاف جنيه ولا تتجاوز 30 الف جنيه او بأحدى هاتين العقوبتين كل من اصطنع بريداً الكترونيا او موقعاً او حساباً خاصاً ونسبه زوراً لشخص طبيعي او اعتباري، فاذا استخدم الجاني البريد او الموقع او الحساب الخاص المصطنع في أمر يسيء الى من نسب اليه تكون العقوبة مدة لا تقل عن سنة وغرامة لا تقل عن 50 الف جنيه ولا تزيد على 200 الف جنيه.

3- جرائم الاعتداء على حرمة الحياة الخاصة

يتمثل هذا النوع من الجرائم في انتهاك الحق في الخصوصية والسرية، فالبيانات الشخصية يمكن الوصول اليها عن طريق زيارة بعض المواقع على شبكة المعلومات، اما انتهاك الخصوصية فيتمثل في الاستخدام غير المصرح به او التوزيع او الكشف عن المعلومات الشخصية مثل

1 - نصت المادة (23) من قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018 على انه (يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر والغرامة التي لا تقل عن ثلاثين الف جنيه ولا تتجاوز خمسين الف جنيه او بإحدى هاتين العقوبتين كل من استخدم الشبكة المعلوماتية او احدى وسائل تقنية المعلومات في الوصول بدون وجه حق الى ارقام او بيانات او بطاقات البنوك، فان قصد من ذلك استخدامها في الحصول على أموال الغير يعاقب بالحبس مدة لا تقل عن 6 اشهر وغرامة لا تقل عن 50 الف جنيه ولا تزيد عن 100 الف جنيه).

السجلات الطبية ,التفضيلات الجنسية ,الوضع المالي وغير ذلك، ويتم ذلك عن طريق اللجوء الى أساليب غير مشروعة للحصول على البيانات الشخصية وبالتالي افشائها.[1]

المطلب الثاني : وسائل الذكاء الاصطناعي في مكافحة الجرائم السيبرانية

مع ارتفاع وتيرة ومقدار الهجمات السيبرانية، فإن التدخل البشري لا يكفي ببساطة لاثبات وتحليل الهجمات في الوقت المناسب، فالحقيقة ان معظم الهجمات الالكترونية تتمحور حول الشبكة التي تتم بواسطة عملاء اذكياء، مثل الفيروسات، وبالتالي لابد من محاربتها بعوامل ذكية شبه مستقلة يمكنها اثبات الهجمات السيبرانية وتقييمها والرد عليه.[2]

بالإضافة الى ذلك فإن الجريمة السيبرانية ليست محلية، بل هي تهديد عالمي لأي نظام كمبيوتر في العالم، وبمعدل متزايد، فلقد كان المتخصصون المتعلمون فقد هم اللذين يرتكبون تلك الجريمة، ولكن اليوم مع توسع شبكات الانترنيت يمكن لأي شخص ان يرتكبها لسهولة الوصول الى المعرفة والأدوات اللازمة لارتكاب هذه الجريمة، وأصبحت الخوارزميات الثابتة التقليدية غير فعالة لاثبات ومكافحة الهجمات الالكترونية المتطورة، لهذا السبب نحتاج الى أساليب مبتكرة مثل تطبيق وسائل الذكاء الاصطناعي التي توفر المرونة والقدرة على التعلم للبرامج التي من شأنها مساعدة البشر في أثبات ومكافحة الجرائم السيبرانية.[3]

ويتمتع الذكاء الاصطناعي بالعديد من الأساليب منها: (الذكاء الحاسبي، الشبكات العصبية ، العملاء المحققين الأذكياء، نظام المناعة الصناعية، تعلم الآلة، تعدين البيانات، التعرف على الأنماط، المنطق الغامض ، الاستدلال...الخ)، وهو ما لعب بشكل متزايد دوراً مهماً في اثبات الجريمة السيبرانية ومكافحتها، ومن خلال الذكاء الاصطناعي يمكننا تصميم حلول الكترونية تلقائية قادرة على التكيف مع سياق استخدامها، وذلك باستخدام أساليب الإدارة الذاتية والتوليف الذاتي والتشخيص الذاتي، وبالتالي يتضح لنا أهمية تقنيات الذكاء الاصطناعي في تحسين التدابير الأمنية للفضاء السيبراني.

من خلال ما تقدم سنحاول بيان وسائل استخدام الذكاء الاصطناعي في سبيل مكافحة الجرائم السيبرانية وكالاتي:

اولاً: استخدام الذكاء الاصطناعي في جمع الأدلة

الاستدلال هو الخطوة التمهيدية التي تسبق تحريك الدعوى الجزائية، ويقوم بها مأموري الضبط القضائي، والغاية من الاستدلال هو جمع الأدلة التي تدخل ضمن إجراءات التحقيق الابتدائي والمحاكمة، وتتميز هذه المرحلة بأهمية كبيرة في كشف الحقيقة[4].

وتتميز مرحلة الاستدلال بعدة خصائص أهمها انها تجري بصورة سرية، كما أنها تتعلق بفرد او بمكان او بشيء معين، وذلك بهدف التعرف على حقيقة الأمور، وبالتالي يجوز لمأمور الضبط

1 - د. محمود رجب فتحي، الوجيز في قانون جرائم تقنية المعلومات المصري ، مصدر سابق، ص157.

2 - R. Stytz , E. Lichtblau , Toward using intelligent agents to detect , assess and counter cyber attacks in network – centric environment, Belvoir Defense Technical Information Center, 2005.

3 - E. Tyugu Artificial intelligence in cyber defense , 3rd International Conference on Cyber Conflict , 2011 , p9.

4 - د. احمد فتحي سرور ، الوسيط في قانون الإجراءات الجنائية ، ط10، دار النهضة العربية، القاهرة، 2016 ، ص331.

القضائي الاستعانة بقواعد البيانات (الوسائل التقنية الحديثة) بمعنى استخدام وسائل الذكاء الاصطناعي في سبيل جمع الأدلة وقد ذكرت محكمة النقض المصري في احد قراراتها : (لا تثريب على رجل هيئة الشرطة ان يصطنع من الوسائل البارعة ما يسلب مقصوده في الكشف عن الجريمة ولا يتصادم مع أخلاق المجتمع)[1].

ويشترط في مرحلة الاستدلال الدقة في دلالتها على ارتكاب الجريمة وبالتالي الدقة في نسبتها للفاعل الأصلي، ولا شك أن الذكاء الاصطناعي يزيد من تلك الدقة، وكذلك يساعد الذكاء الاصطناعي في تجميع الأدلة بصورة سريعة وكذلك الدقة في المعاينة وتحديد الحالة الصحية والنفسية والعقلية وهذا ما يتم تداركه عن استخدام الذكاء الاصطناعي.[2]

ويمكن استخدام الذكاء الاصطناعي في مكافحة الجريمة من خلال معاينة مسرح الجريمة بواسطة نظام تحديد المواقع (GPS) حيث يعمل هذا النظام من خلال التقاط إشارات تطلق من الأقمار الاصطناعية التي تدور حول الأرض، وبواسطة هذا النظام يمكن تحديد موقع في الصحراء او وسط البحار والمحيطات، ويكمن الاستفادة ايضاً منه في إعادة معاينة مسرح جريمة وقعت في الصحراء مثلاً بعد ان تغيرت معالم المنطقة بسبب الكثبان الرملية، وبالتالي إمكانية إعادة معاينة مسرح الجريمة بسبب صعوبة تحديد الوصول اليها وذلك باستخدام وسائل الذكاء الاصطناعي.[3]

ومن التطبيقات العملية في مجال الجريمة السيبرانية في صورة تعقب حركة البيانات على الأنترنيت حيث اعتقل (فاسيلي جوركوف و أليكسي إيفانون) لاحقاً في الولايات المتحدة الامريكية في عام 2000 وتوقع المحققون ان يكونا من زعماء عصابات الجريمة المعلوماتية الروس الذي اخترقو شبكات لا تقل عن 40 شركة أمريكية ثم حاولوا ابتزاز المال.[4]

ومن وسائل الذكاء الاصطناعي هو القياس الحيوي للبصمة الوراثية (تحليل DNA) وكان القضاء الجنائي قد توسع في استخدام هذه التقنية وذلك في حوادث التفجيرات الإرهابية والتي لم يكن بالأمكان التعرف على هويات الضحايا الا عن طريق فحص الحمض النووي، وقد كان لهذه التقنية الدور الكبير في منع التلاعب من قبل ضعاف النفوس في تقديم ادعاءات باطلة في سبيل الحصول على التعويضات، وكذلك كان لهذه التقنية دور مهم في تحديد المحكمة المختصة مكانياً او نوعياً، ومثلت انعاطفاً مهما نحو تطور القانون الجنائي، حيث يستخدم الذكاء الاصطناعي عند تحليل الحمض النووي لينتج كميات كبيرة من البيانات المعقدة في شكل الكتروني، تحتوي هذه البيانات على أنماط بعضها قد يستحيل تحليله من قبل العقل البشري.[5]

1 - قرار محكمة النقض المصري الطعن رقم 2026 لسنة 48 جلسة 1979/4/8 س30 ع1 ص453 ق96.
2 - سعود محمد موسى ، التحريات (ماهيتها ، طبيعتها القانونية ، سندها)، مجلة الفكر الشرطي ، يصدرها مركز بحوث شرطة الشارقة ، الامارات، مجلد7، ع 4، 1999، ص157.
3 - د. تامر محمد صالح، التتبع الجغرافي للمتهم بواسطة تقنية GPS كأحد إجراءات جمع الأدلة، دار الفكر والقانون ، المنصورة ، 2021، ص16.
4 - د. محمود رجب فتح الله ، البصمة الرقمية ودورها في الاثبات الجنائي، دار الجامعة الجديدة، الإسكندرية، 2021، ص80ومابعدها.
5 - Faya Mitchell, The use of artificial intelligence in digital forensics: an introduction, Digital Evidence and Electronic Signature Law Review, Vol 7, 2016 , p37.

ثانياً: استخدام الذكاء الاصطناعي في اثبات التلبس بالجريمة

التلبس هو حالة يتم فيها مشاهدة الجريمة حال ارتكابها او عقب ارتكابها بوقت يسير[1]، حيث يتم اثبات التلبس باستخدام وسائل الذكاء الاصطناعي ومنها كاميرات المراقبة او مراقبة الهاتف المحمول او أي نشاط الكتروني (مواقع التواصل الاجتماعي)، فيتم من خلالها مراقبة الأشخاص المشتبه بهم او مراقبة أماكن يمنع الدخول اليها في أوقات معينة او أماكن يحظر الدخول اليها وهنا ترسل برامج الذكاء الاصطناعي تنبيهات الى الشخص المختص اذا اكتشفت ان هناك شخصاً ينتهك تلك الحماية بتواجده في تلك الأماكن او خلال تلك الأوقات، وتتميز هذه البرامج بقدرتها على اكتشاف على اكتشاف التعدي في حالات تتجاوز القدرة البشرة كما في حالة المسافات الكبيرة او اثناء الأمطار كما تمكن هذه الوسيلة متابعة أشخاص محددين من خلال مئات الكاميرات في آن واحد، وتسهل إعادة بناء مسرح الجريمة وتظهر كل محتويات المكان حتى ما لا تراه العين المجردة كبقعة الدم، كما انها تحتفظ بصورة الجثث التي قد يكتشف برنامج لاحق تفاصيل دقيقة كانت تختفي بعد دفن الجثة.[2]

ثالثاً: استخدام الذكاء الاصطناعي في تفتيش البيئة الرقمية

التفتيش هو إجراء من إجراءات التحقيق الابتدائي، ويقصد به البحث عن الأدلة المادية لجريمة وقت في مكان ذي حرمة كالمسكن، او لدى شخص، وغايته اثبات ارتكاب الجريمة او اثبات نسبتها الى متهم.[3]

اما تفتيش البيئة الرقمية فهو البحث في مستودع سري للمتهم ذو حماية خاصة مثل (الكمبيوتر ، الانترنيت) عن الأدلة المادية والمعنوية في سبيل الكشف عن الحقائق ونسبتها الى الجاني، والتفتيش اجراء من إجراءات التحقيق الابتدائي ويجب تدوينه وعدم افشاء اسراره، وقد نص قانون مكافحة جرائم تقنية المعلومات المصري على جواز تفتيش البيئة الرقمية متى كان لذلك فائدة في ظهور الحقيقة على ارتكاب جريمة معاقب عليها وفق احكام ذلك القانون، وهو ما يعني ضرورة وقوع جريمة سيبرانية او على الأقل توافر معلومات عن احتمال وقوع مثل تلك الجريمة.[4]

ويشمل تفتيش البيئة الرقمية تفتيش الأجهزة وملحقاتها المادية، وفي حالة كونها في حيازة صاحبها فتعتبر امتداداً له، ومن ثم لا يجوز تفتيشها الا في الحالات التي يجوز فيها تفتيش الأشخاص وبالضمانات والقيوم المقررة في القانون، اما في حالة كونها في مكان خاص كسكن المتهم او أحد ملحقاته فتأخذ حكمه، فلا يجوز تفتيشها الا في حالات جواز تفتيش مكسن المتهم وبالضمانات والقيود المنصوص عليها.[5]

1 - د. عمر سالم ، الوجيز في شرح قانون الإجراءات الجنائية، ج1، دار النهضة العربية ، القاهرة ، 2021، ص156.

2 - Lenin Mookiah, William Eberle, Ambareen Siraj, Survey of Crime Analysis and Prediction, Proceedings of the twenty-eighth International Florida Artificial Intelligence Research Society Conference, 2015, p37.

3 - د. احمد فتحي سرور ، الوسيط في قانون الإجراءات الجنائية ، مصدر سابق ، ص345.

4 - ينظر : المادة (6) من قانون مكافحة جرائم تقنية المعلومات المصري رقم (175) لسنة 2018.

5 - سوسن سعيد، دليل الاثبات الالكتروني ، بحث منشور في مجلة جامعة شندي ، السودان، ع11، 2011، ص131.

الخاتمة

في نهاية هذا البحث الموسوم بـ (استخدام الذكاء الاصطناعي في مكافحة الجرائم السيبرانية توصلنا الى عدد من النتائج والتوصيات نوجزها بالآتي:

اولا: النتائج

1. أن الجريمة السيبرانية لا تختلف عن الجرائم التقليدية التي ينص عليها قانون العقوبات، فهي تتطلب وجود عناصر محددة يجب توافرها في أي جريمة، وهذا يشمل الجرائم السيبرانية كجزء من القوانين الجنائية العامة، هذا النوع من الجرائم يتطلب وجود ركنين أساسيين: ركن مادي وركن معنوي.
2. تتنوع الجرائم السيبرانية فيمكن ان يتم من خلالها ارتكاب اعمال السرقة والاحتيال والتزوير والتشهير والحاق الأذى والاختراق وجرائم القرصنة وكذلك جرائم انشاء مواقع الكترونية وايضاً الاعتداء على المواقع الرسمية للدولة وقرصنة معلوماتها.
3. من خلال الذكاء الاصطناعي يمكننا تصميم حلول الكترونية تلقائية قادرة على التكيف مع سياق استخدامها، وذلك باستخدام أساليب الإدارة الذاتية والتوليف الذاتي والتشخيص الذاتي.
4. نستطيع من خلال وسائل الذكاء الاصطناعي مكافحة الجريمة وذلك عن جمع الأدلة بواسطة الذكاء الاصطناعي ، القيام بعملية التفتيش الرقمي ، وكذلك استخدام الذكاء الاصطناعي في اثبات التهمة على الجاني.

التوصيات:

1. نوصي الجهات المختصة على ضرورة الإسراع في إقرار مشروع قانون جرائم المعلوماتية العراقي هذا المشروع الضرورة لمكافحة الجرائم السيبرانية والتي انتشرت في الآونة الأخيرة منها جريمة اختراق المواقع الرسمية مثل موقع اور وحذف الكثير من المخالفات المرورية وغيرها من الجرائم.
2. نوصي الحكومة العراقي في إيلاء الاهتمام الخاص بخريجي كليات واقسام الذكاء الاصطناعي لما لهم من دور في دعم المؤسسات الرسمية وغير الرسمية وتوظيفهم وتطوير قدراتهم.
3. نوصي بضرورة تكثيف الدراسات الخاصة بأستخدام الذكاء الاصطناعي وكذلك الدراسات الخاصة بالجريمة السيبرانية وطرق اثباتها وكذلك مكافحتها.
4. تثقيف وتأهيل الأجهزة المختصة لتطوير مهاراتهم ومعلوماتهم فيما يخص الجرائم السيبرانية وكذلك تطبيقات الذكاء الاصطناعي من خلال تكثيف الدورات الخاصة.

المصادر والمراجع

أولا: المؤلفات

1. احمد فتحي سرور ، الوسيط في قانون الإجراءات الجنائية ، ط10، دار النهضة العربية، القاهرة، 2016 .
2. الآن بونية : الذكاء الاصطناعي ،ترجمة د. صبري فرغلي ، سلسلة عالم المعرفة ، المجلس الوطني للثقافة والفنون والآداب ، الكويت ، 1993.

3. بلال أمين زين الدين: جرائم نظم المعالجة الالية للبيانات ، دار الفكر الجامعي ، الاسكندرية، 2008.

4. تامر محمد صالح، التتبع الجغرافي للمتهم بواسطة تقنية GPS كأحد إجراءات جمع الأدلة، دار الفكر والقانون، المنصورة ، 2021 .

5. سعود محمد موسى ، التحريات (ماهيتها ، طبيعتها القانونية ، سندها)، مجلة الفكر الشرطي ، يصدرها مركز بحوث شرطة الشارقة ، الامارات، مجلد7، ع 4، 1999.

6. عباس الحسني، شرح قانون العقوبات العراقي الجديد، المكتبة القانونية ، بغداد، بدون سنة

7. عبد الله موسى ، د. احمد حبيب بلال، الذكاء الاصطناعي ثورة في تقنيات العصر، القاهرة ، المجموعة العربية للتدريب والنشر، 2019 .

8. علي حسين الخلف ، د. سلطان عبد القادر الشاوي ، المبادئ العامة في قانون العقوبات ، العاتك لصناعة الكتاب ، القاهرة ، ط2 ، 2010.

9. عمر سالم ، الوجيز في شرح قانون الإجراءات الجنائية، ج1، دار النهضة العربية ، القاهرة ، 2021.

10. محمود رجب ، شرح قانون مكافحة جرائم تقنية المعلومات في ضوء القانون المصري، 175 لسنة 2018 ، دار الفكر الجامعي ، الإسكندرية.

11. محمود رجب فتح الله ، البصمة الرقمية ودورها في الاثبات الجنائي، دار الجامعة الجديدة، الإسكندرية، 2021.

12. محمود سعد عبد المجيد ، الجرائم السيبرانية وانعكاسات ثورة التكنولوجيا على النظرية العامة للجريمة ، دار المطبوعات الجامعية ، الإسكندرية ، 2023.

13. محمود سعد عبد المجيد ، الجرائم السيبرانية وانعكاسات ثورة التكنولوجيا على النظرية العامة للجريمة ، دار المطبوعات الجامعية ، الإسكندرية ، 2023.

14. ممدوح عبد الحميد عبد المطلب ، جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية ، دار الفتح للطباعة والنشر، الامارات، 2000.

15. منال البلقاسي ، الذكاء الاصطناعي صناعة المستقبل ، دار التعليم الجامعي ، الإسكندرية ، 2019.

16. هبة ممدوح إبراهيم ، الجوانب الإجرائية لجرائم الانترنيت، دار الفكر الجامعي ، الإسكندرية ، 2019.

ثانياً: الاطاريح والرسائل

1. سارة أمجد عبد الهادي ، الذكاء الاصطناعي في ظل القانون الجزائي ، أطروحة دكتوراه ، كلية الدراسات العليا ، جامعة القدس ، فلسطين ، 2022.

2. عمار ياسر زهير البابلي ، الآليات الحديثة لحماية وتأمين نظم المعلومات وآثارها على المنظومة الأمنية ، رسالة دكتوراه ، كلية الدراسات العليا ، اكادمية الشرطة ، القاهرة، 2018.

3. غادة المنجم: الذكاء الاصطناعي وعلاقته بنظم مساندة القرار، رسالة ماجستير ، كلية العلوم الإدارية، جامعة الملك سعود، الرياض، 2012.

ثالثاً: البحوث والمقالات

1. دعاء حاتم ، لمى العزاوي، الذكاء الاصطناعي والمسؤولية الجنائية الدولية بحث منشور في مجلة المفكر ، كلية الحقوق والعلوم السياسية ، جامعة محمد بسكرة ، الجزائر، ع 18 ، 2006

2. عماد الدحيات ، نحو تنظيم قانوني للذكاء الاصطناعي في حياتنا، بحث منشور في مجلة الاجتهاد للدراسات القانونية والاقتصادية، كلية القانون، جامعة الامارات العربية المتحدة، المجلد 8، ع5 ، 2019.

3. محمود مختار ، تطبيقات الذكاء الاصطناعي، بحث منشور في المجلة الدولية في العلوم التربوية ، المؤسسة الدولية لآفاق المستقبل ، مجلد3، ع4، 2020.

القوانين

-1 مشروع قانون جرائم المعلوماتية العراقي لسنة 2011.

-2 قانون جرائم المعلوماتية المصري رقم (175) لسنة 2018.

-3 القانون رقم (34) لسنة 2021 الخاص في مكافحة الشائعات والجرائم الالكترونية الاماراتي.

المؤلفات باللغة الأجنبية

1. D.Dasgupta, Computational Intelligence in Cyber Security , IEEE International Conference on Computational for Homeland Security and Personal Safety , 2006 .

2. E. Tyugu Artificial intelligence in cyber defense , 3rd International Conference on Cyber Conflict , 2011 .

3. Faya Mitchell, The use of artificial intelligence in digital forensics: an introduction, Digital Evidence and Electronic Signature Law Review, Vol 7, 2016 .

4. George F. Luger , Artificial Inteligence ; Structures and Strategies for Complex Problem Solving , Addison – Wesley , 2002.

5. Lenin Mookiah, William Eberle, Ambareen Siraj, Survey of Crime Analysis and Prediction, Proceedings of the twenty-eighth International Florida Artificial Intelligence Research Society Conference, 2015.

6. R. Stytz , E. Lichtblau , Toward using intelligent agents to detect , assess and counter cyber attacks in network – centric environment, Belvoir Defense Technical Information Center, 2005.