دور الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية

دراسة مقارنة

The Role of Artificial Intelligence in Combating Cybercrime
A Comparative Study

أ مراد محمد غالب محمد قاسم

مساعد باحث بجامعة الجند للعلوم والتكنولوجيا/ طالب ماجستير/ جامعة تعز، (اليمن)

qqyuip3@gmail.com

تاريخ الاستلام: 17-02-2024 تاريخ القبول: 26-04-2024 تاريخ النشر: 01-06-2024

DOI: https://doi.org/10.70411/MJLS.2.2.202495

الملخص:

تُعَدُّ الجرائم الإلكترونية من أخطر الجرائم التي تواجه الأفراد والمؤسسات؛ كونها جرائم صامتة تتجاوز الحدود الجغرافية؛ حيث تستخدم شبكة الإنترنت وأجهزة الحاسوب في تنفيذ أعمال إرهاب إلكتروني واختراق وقرصنة البيانات، ومع ذلك لم تدم هذه الجريمة لفترة طويلة حتى ظهرت تقنية الذكاء الاصطناعي ذات المستوى العالي كحاجز لمكافحة الجرائم الإلكترونية، خاصة في الدول المتقدمة؛ فعن طريق السلطات الرقمية وتوقعات الجريمة قبل وقوعها ووسائل أخرى ساهم الذكاء الاصطناعي بشكل كبير في مكافحة الجريمة الإلكترونية، وانقسمت التشريعات العربية بين من يعمل على تنظيم قوانين خاصة بالجرائم الإلكترونية وبين من قام بتعديل القوانين القديمة لمواكبة التطورات الحاصلة في مبدأ مشروعية مكافحة الجرائم الإلكترونية.

تهدف هذه الدراسة إلى معرفة دور الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية، وكيف ساهمت السلطات الرقمية وتقنيات التنبؤ بالجرائم في منع وتقليل الجرائم الإلكترونية؟ وما هو دور بعض التشريعات العربية في تنظيم مكافحة الجريمة الإلكترونية والآلية المتبعة لمواجهتها؟

ولتحقيق أهداف الدراسة استخدم الباحث المنهج الوصفي التحليلي لمعرفة آلية استخدام الذكاء الاصطناعي في مواجهة الجريمة الإلكترونية، والمنهج المقارن من خلال المقارنة بين الأنظمة القانونية ودورها في مكافحة الجريمة الإلكترونية.

الكلمات المفتاحية: الذكاء الاصطناعي، الجرائم الإلكترونية، الشرطة الرقمية، الإرهاب الإلكتروني.

Abstract:

Cybercrimes are among the most dangerous crimes facing individuals and institutions, as they are silent crimes that transcend geographical boundaries. The Internet and computer devices are used to execute acts of cyber terrorism, hacking, and data piracy. However, these crimes did not persist for long until the high-level artificial intelligence technology emerged as a barrier to combating cybercrimes, especially in developed countries.

Through digital authorities, crime prediction before it occurs, and other means, artificial intelligence has significantly contributed to combating cybercrimes. Arab legislations have been divided between those who working on regulating specific laws for cybercrimes and those who have amended old laws to keep pace with the developments in the principle of the legitimacy of combating cybercrimes.

This study aims to understand the role of artificial intelligence in combating cybercrimes, and how digital authorities and crime prediction techniques have contributed in preventing and reducing cybercrimes.

It also examines the role of some Arab legislations in regulating the fight against cybercrimes and the mechanism adopted to combat them.

To achieve the objectives of the study, the researcher utilized the descriptive-analytical approach to explore the mechanism of using artificial intelligence in combating cybercrimes, and the comparative approach by comparing the legal systems and their role in combating cybercrime.

Keywords: Artificial Intelligence, Cybercrimes, Digital Police, Cyber Terrorism.

المقدمة:

يُعد الذكاء الاصطناعي من المصطلحات التي ظهرت مؤخرًا، حيث أصبح الذكاء الاصطناعي يشهدُ تطورًا ملحوظًا في السنوات الأخيرة، ولعبَ دورًا مهمًا في شتى مجالات الحياة المختلفة القانونية والطبية والهندسية، وكان للذكاء الاصطناعي دور بارز في مكافحة الجرائم المستحدثة، ويمكن للذكاء الاصطناعي إن بُرمجَ لمكافحة ومواجهة مخاطر جرائم معينه مثل الجرائم الإلكترونية أن يقوم بذلك، حيث عملت أغلب الدول المتقدمة على استخدام الذكاء الاصطناعي في مواجهة الجرائم الإلكترونية، أما بالنسبة للدول العربية فقد انقسمت بين من واكب التشريع القانوني بالتقدم التكنولوجي، واستخدم وسائل الذكاء الاصطناعي لمواجهة الجرائم الإلكترونية، وبين من ذهبت إلى تعديل بعض القوانين لتواكب التقدم الحديث لمكافحة الجرائم الإلكترونية، لكنها ماتزال تعمل بطرق بدائية لمواجهة خطر الجرائم الإلكترونية، وهذا ما سنتناوله في دراستنا هذه.

أهمية البحث:

تتمثل أهمية هذه الدراسة في تطور الذكاء الاصطناعي الجدي والحيوي، وهو دور الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية دراسة مقارنة بين القوانين العربية، ومن هذا المنطلق يمكن تقسيم أهمية البحث إلى قسمين: الأهمية النظرية والأهمية العلمية كالآتي:

الأهمية النظرية: من خلال الإحاطة بمفهوم وخطورة الجرائم الإلكترونية، والكشف عن إمكانية استغلال الذكاء الاصطناعي في مكافحة هذه النوعية من الجرائم المستحدثة في العصر الحديث.

الأهمية العلمية: من خلال التوصيات التي سيوصي بها الباحث، والتي يمكن الاستفادة منها لوضع أسس وتفعيل المفاهيم الجديدة؛ لتفعيل الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية المستحدثة.

مشكلة البحث:

تكمن مشكلة البحث في ظهور أنماط جديدة من الجرائم الإلكترونية الحديثة التي تُرتكب عبر أجهزة الحاسوب، وتُعد من أهم التحديات الأمنية التي تواجه المجتمع؛ حيث إن أغلب المجرمين يتبعون وسائل التقنية الحديثة لارتكاب الجرائم، لذلك لا بُد من معرفة دور الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية، والتصدي لها، ومعرفة مرتكبيها، ومواكبة التشريعات والقوانين الناظمة لها، وبناءً على ذلك تتمثل مشكلة البحث في الآتي:

1. ما مفهوم الذكاء الصناعي والجريمة الإلكترونية؟
2. ما دور الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية وموقف التشريعات القانونية منها؟

أهداف البحث:

بناءً على مشكلة الدراسة والتساؤلات المطروحة فيها تهدف الدراسة إلى الآتي:

1. التعرف على ماهية الذكاء الاصطناعي والجريمة الإلكترونية.
2. معرفة دور الذكاء الاصطناعي في مكافحة الجريمة وموقف التشريعات القانونية منها.

منهجية البحث:

تم الاعتماد في هذه الدراسة على المنهج الوصفي التحليلي من خلال معرفة ماهية الذكاء الاصطناعي والجريمة الإلكترونية، وماهية دور الذكاء الاصطناعي في مكافحة الجريمة، والمنهج المقارن من خلال معرفة موقف التشريعات العربية من دور الذكاء الاصطناعي في مواجهة الجريمة الإلكترونية.

خطة البحث:

تم تقسيم البحث الى المطلبين الآتيين :

المطلب الأول: ماهية الذكاء الاصطناعي والجريمة الإلكترونية.

المطلب الثاني: دور الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية وموقف التشريعات القانونية العربية منها.

المطلب الأول :

ماهية الذكاء الاصطناعي والجريمة الإلكترونية

يُعد الذكاء الاصطناعي سلاحًا فعالًا ذو حدين يمكن استخدامه في مكافحة الجريمة وتعقب المجرمين، ويمكن استخدامه في عملية تطوير الجريمة الإلكترونية[1]، وتوجد علاقة ارتباط بين الذكاء الاصطناعي وبعض الجرائم الإلكترونية المستحدثة، لاسيما فيما يتعلق بالحاسب الآلي الذي يستخدم كآلية لعملية الجرائم الإلكترونية[2]؛ لذلك سنتطرق للتعرف على مفهوم الذكاء الاصطناعي في فرع أول ومفهوم الجريمة الإلكترونية في فرع ثانٍ.

الفرع الأول :

ماهية الذكاء الاصطناعي

يُعد الذكاء الاصطناعي من الوسائل الحديثة التي يتم الاعتماد عليها في مجالات عدة، منها مكافحة الجرائم الإلكترونية التي يقوم بها كثير من المجرمين في العالم، وسنسلط الضوء –هنا– على تعريف الذكاء الاصطناعي وأهميته وأهدافه وخصائصه في النقاط الآتية:

أولًا : تعريف الذكاء الاصطناعي

لمعرفة الذكاء الاصطناعي لا بُد من معرفة الذكاء الإنساني الذي يربط القدرة العقلية في التكيف على الظروف المحيطة بالإنسان، والاستفادة من التجارب والخبرات السابقة، والتفكير والتخطيط وحل المشاكل والقدرة على الاستنتاج[3].

أما بالنسبة للذكاء الاصطناعي فيُعَرف أنه: "الآلات المخترعة بطريقة يدوية تحاكي ذكاء الإنسان"[4].

---

[1]. رانا مصباح عبد المحسن عبد الرزاق، دور الذكاء الاصطناعي في مواجهة جرائم الإرهاب الإلكتروني، المجلة الأكاديمية لجامعة نورا، الرياض، 2023م، ص15.

[2]. الأخنش نورة أمينة، العيداني محمد، الذكاء الاصطناعي كآلية لمجابهة الجريمة الإلكترونية، مجلة القانون والعلوم البيئية، المجلد2، العدد2، 2023م، ص529.

[3]. الذكاء الصناعي، مركز البحوث العربية، لسنة 2021م، ص5.

[4]. الأخنش نورة أمينة، العيداني محمد، المرجع السابق، ص529.

وقد عَرَّف البعض الذكاء الاصطناعي أنه: "أنظمة تستخدم تقنيات قادرة على جمع البيانات واستخدامها للتنبؤ أو التوصية أو اتخاذ القرار– بمستويات متفاوتة من التحكم الذاتي– واختيار أفضل إجراء لتحقيق أهداف محددة"[1].

ومنهم من عرفه أنه: "جزء من علوم الحاسب الآلي الذي يهدف إلى محاكاة قدرة معرفية لاستبدال الإنسان في أداء وظائف مناسبة في سياق معين تتطلب الذكاء"[2].

ويُعَرف الذكاء الاصطناعي أنه: "دراسة وتصميم أنظمة ذكية تستوعب بيئتها، وتتخذ إجراءات تزيد من فرص نجاحها"، في حين يعرفه جون مكارثي أنه: "علم وهندسة صنع الآلات الذكية"[3].

ويُعَرف أنه: "مجموعة من السلوكيات التي تتسم بها البرامج الحاسوبية، ويكون الهدف منها تقوية القدرة الإنتاجية من جهة العمل على محاكاة القدرات الذهنية البشرية من جهة أخرى" [4].

ويُعَرف أنه: "ذلك الفرع من علوم الحاسوب الذي يمكن بواسطته خلق وتصميم برامج الحاسبات التي تحاكي أسلوب الذكاء الإنساني؛ لكي يتمكن الحاسب من أداء بعض المهام بدلًا عن الإنسان، والتي تتطلب قيام الحاسب الآلي بالتفكير والتفهم والسمع والتكلم والحركة بأسلوب منطقي ومنظم" [5].

ثانيًا: أهمية الذكاء الاصطناعي

يلعب الذكاء الاصطناعي دورًا مهمًا في المجال الإداري والمحاسبي والإلكتروني، ويقوم بحل المشاكل والمسائل المحاسبية والإدارية والأعمال الصناعية [6]، ويعمل على تخفيف الكثير من المخاطر والضغوطات النفسية على الإنسان خاصةً في الميادين التي تتضمن تفاصيل تتسم بالتعقيد وتحتاج إلى تركيز عقلي

---

[1]. عبد الله شرف الغامدي، الهيئة السعودية للبيانات والذكاء الاصطناعي، سلسلة الأدلة الإرشادية1، السعودية، 2022م، ص8.

[2]. الأخنش نورة أمينة، العيداني محمد، المرجع السابق، ص530.

[3]. سعود عبد القادر الشاعر، دور الذكاء الاصطناعي في تفعيل إجراءات التحقيق الجنائي في الجرائم الإلكترونية (دراسة مقارنة)، الإمارات العربية المتحدة، جامعة عجمان، 2020م، ص11.

[4]. رانا مصباح محسن، المرجع السابق، ص15 وما بعده

[5]. عبدالله أحمد مطر الفلاسي، المسؤولية الجنائية الناتجة عن أخطاء الذكاء الاصطناعي، المجلة القانونية، مجلة متخصصة في الدراسات والبحوث القانونية، دون دار نشر، دون سنة نشر، ص8.

[6]. الأخنش نورة أمينة، العيداني محمد، المرجع السابق، ص530.

متعب وحضور ذهني متواصل[1]، وله دور كبير في التحري والتحقيق في الجرائم الإلكترونية ومواجهتها من خلال مراقبة الاتصالات الرقمية والشبكة العنكبوتية، واكتشاف الجرائم قبل وقوعها[2]، وتبرز أهمية الذكاء الاصطناعي من خلال إدخال النظام الذكي في كاميرات المراقبة لإرسالها إلى الشرطة في حال وجود شخص يتصرف بطريقة غير طبيعية، ولذلك يعمل على المساهمة في الحد من الجرائم الإلكترونية ومكافحتها بشكل مستمر وفعال.

ثالثًا: أنواع الذكاء الاصطناعي

مع تقدم الذكاء الاصطناعي يمكن تقسيمه من حيث النطاق إلى عدة أقسام كما يأتي:

1. الذكاء الاصطناعي الضيق، وهو: الذكاء الذي يعمل وفق برمجة معينة ومحددة مسبقًا، ولا يمكن أن يتعداها[3]، على سبيل المثال: تصنيف البريد الإلكتروني كرسائل غير مرغوب فيها، أو أنه ليس عشوائيًا.
2. الذكاء الاصطناعي بالمعنى الواسع، وهو الذي لديه القدرة على جمع المعلومات وتحليلها، ويتمكن من اكتساب المهارات والقدرات والعمل بصفة مستقلة وذاتية[4]، كما يمكن أن يؤدي الدور الذي يقوم به الإنسان[5].
3. الذكاء الاصطناعي الفائق، وهو الذي يفوق قدرات الإنسان [6]، ويُعَرفه الفيلسوف في جامعة أكسفورد، نيك بوستروم أنه: "فكر أذكى بكثير من أفضل العقول البشرية في كل مجال تقريبًا، بما في ذلك الإبداع العلمي والحكمة العامة والمهارات الاجتماعية".

---

[1]. أروى بنت عبد الرحمن الجلعود، أحكام تطبيقات الذكاء الاصطناعي في القضاء، السعودية، الطبعة الأولى، 1444هـ، ص46.

[2]. رانا مصباح محسن، المرجع السابق، ص17.

[3]. رانا مصباح محسن، المرجع السابق، ص17.

[4]. المرجع نفسه.

[5]. نقلاً عن. الأخنش نورة أمينة، العيداني محمد، المرجع السابق، ص531.

رابعاً: خصائص الذكاء الاصطناعي

1. التعلم الآلي والمستمر :أي التعلم من المشكلات والاستفادة من مختلف الخبرات السابقة[1].
2. اتخاذ القرار: لديه القدرة على اتخاذ القرار بناءً على القواعد والبيانات الاحتمالية[2].
3. القدرة: من خلال استخدام التجربة الخطأ لاستكشاف الأمور المختلف عليها، مع زيادة قدرة الاستجابة السريعة للمواقف والظروف الجديدة والمختلفة والحالات الصعبة والمعقدة[3].
4. الإبداع: يمكن له أن يولد أفكارًا وابتكارات جديدة في شتى المجالات المختلفة[4].

الفرع الثاني:

الجرائم الإلكترونية

يُعد ظهور الأجهزة الإلكترونية والإنترنت ذا خطورة عالية خاصة في ظل انتشار الجريمة الإلكترونية المنظمة والتي تتجاوز حدود الدول، وتستطيع اختراقها، وأخذ المعلومات الخاصة بها، ولا تقف الجريمة الإلكترونية عند ذلك الحد، وإنما تتجاوز ذلك إلى مستوى خصوصية حياة الأفراد، بل إن أغلب عملية الاغتيالات والنصب والاحتيال والسرقات تتم عن طريق استخدام أجهزة الحاسوب وتقنية الإنترنت، ومن هنا سيتم التعرف في هذا الفرع عن ماهية الجريمة الإلكترونية وخصائصها وخطورتها للفرد والمجتمع كما يلي: –

أولًا: ماهية الجريمة الإلكترونية

اختلف فقهاء الأنظمة القانونية حول تعريف الجريمة الإلكترونية، وذلك حسب الزاوية التي تعالجها أو الجهة التي تنظر إليها، فمنهم من ذهب إلى التوسع في تعريف الجريمة الإلكترونية، ومنهم من ذهب إلى تضييق مفهوم الجريمة الإلكترونية، فالفريق الذي يُضيق من الجريمة الإلكترونية عرفها أنها: "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف المعلومات، أو الوصول إلى المعلومات المخزنة داخل الحاسب

---

[1] . المرجع نفسه.

[2] .رشا محمد صائم، تطبيقات الذكاء الاصطناعي في اتخاذ القرارات الإدارية، رسالة مقدمة لاستكمال متطلبات درجة الماجستير، جامعة الشرق الأوسط، 2022م، ص26.

[3] .عمار ياسر زهير البابلي، دور أنظمة الذكاء الاصطناعي في التنبؤ بالجريمة، مجلة الأمن والقانون، أكاديمية دبي للنشر، الإمارات، المجلد 29، العدد1، 2021، ص141. ص

[4] . المرجع نفسه.

الآلي أو تلك التي يتم تحويلها عن طريقه"[1]، ومنهم من عرفها أنها: "الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي"[2]، أما الاتجاه الموسع في تعريف الجريمة الإلكترونية فقد ذهب إلى أنها: "سلوك إجرامي يتم بمساعدة الكمبيوتر"، ومنهم من قال إنها: "كل جريمة تحيط في أجهزة الكمبيوتر"[3]، وقد ذهب فريق آخر إلى أنها: "كل فعل إجرامي يستخدم الحاسب الآلي في ارتكابه كأداة رئيسية"[4].

أما بالنسبة للتعريفات القانونية للجريمة الإلكترونية فقد عرفها المشرع الأمريكي أنها: "الاستخدام غير المصرح به لأنظمة الكمبيوتر المحمية، أو ملفات البيانات، أو الاستخدام المتعمد الضار لأجهزة الكمبيوتر، أو ملفات البيانات، وتتراوح خطورة تلك الجريمة ما بين جناية من الدرجة الثانية إلى جناية من الدرجة الثالثة"[5].

وقد عَرَّفها المشرع الفلسطيني أنها: "سلوك إنساني يرتكب بواسطة حاسب آلي، إخلالاً بقواعد القانون الجنائي؛ يترتب عليه المساس بمصلحة يحميها الشارع، ويوقع القضاء بحكم قضائي بات على مرتكبه الجزاء المناسب"[6].

ويرى الباحث بأن التعريفات السابقة ليست شاملة جامعة لتعريف الجرائم الإلكترونية؛ إذ إن أغلب الفقهاء حصروا الجرائم الإلكترونية في أجهزة الكمبيوتر(الحاسب الآلي، ولم يتم التطرق إلى بقية الأجهزة الإلكترونية الحديثة التي تستخدم في ارتكاب جرائم معينة، وكذا انتهاك خصوصية المجني عليه دون مراعاة للحدود الجغرافية لاسيما جرائم الأجهزة المحمولة، وهناك قوانين لم تسلك تنظيم الجرائم الإلكترونية بعد، رغم أن هذه الجرائم تخالف العادات السائدة في المجتمع، ولو لم تكن مخالفة بصريح القانون، ومن خلال

---

[1]. الجرائم الإلكترونية، إعداد اللجنة العلمية بمعهد الكويت للدراسات القضائية والقانونية، 2019م، ص8.

[2]. سميرة معاشي، ماهية الجريمة المعلوماتية، مجلة المنتدى القانوني، جامعة محمد خضير بسكرة، العدد السابع، دون سنة نشر، ص277.

[3]. المرجع نفسه، ص277.

[4]. الجرائم الإلكترونية، إعداد اللجنة العلمية بمعهد الكويت للدراسات القضائية والقانونية، مرجع سابق، ص9.

[5]. نقلاً عن إيمان يوسف صبرة، حقوق المجني عليه في الجرائم الإلكترونية في التشريع الفلسطيني: دراسة مقارنة مع القانون والشريعة الإسلامية، رسالة مقدمة لأستكمال متطلبات الحصول درجة الماجستير، الجامعة الإسلامية بغزة، فلسطين، 2020م، ص11.

[6]. المرجع نفسه، ص14.

ذلك يعرف الباحث الجريمة الإلكترونية أنها: كل سلوك منظم وغير منظم تستخدم من خلاله الأجهزة الإلكترونية كافة في ارتكاب جرائم يعاقب عليها القانون أو تكون مخالفة للعرف المجتمعي.

ثانيًا: خصائص الجريمة الإلكترونية

تتسم الجرائم الإلكترونية بأنها جريمة حديثة وخطيرة، ظهرت مع ظهور التقدم التكنولوجي في العصر الحديث، وهي جريمة عابرة للقارات، ولا تقف عند الحدود الجغرافية للدول، ولذلك سوف نتعرف عن خصائص الجريمة الإلكترونية كما يأتي:

1- خطورة الجريمة الإلكترونية:

تتسم الجريمة الإلكترونية بأنها جريمة تمس الحياة الخاصة للأفراد والمؤسسات، ومن شأن ذلك أن يترتب عليه خسائر غير مسبوقة باقتصاد الدول، فالجريمة الإلكترونية لا تحتاج إلى جهد عضلي، بل تحتاج إلى نوع من الذكاء والدراية الذهنية[1]؛ فلا يمكن لشخص أن يرتكب الجريمة الإلكترونية دون وعي بتقنيات الحاسب الآلي والأجهزة الحديثة[2]، وتبرز خطورة هذه الجريمة في إمكانية ارتكابها بشكل ناعم، فلا يشترط وجود المجرم في مسرح الجريمة وإنما يمكن تنفيذها عن بُعد، كما أنها تعود على المجرمين بفوائد مالية كبيرة، لذلك تُعد الجريمة نوعًا من الإغراء للمجرمين لاستغلال التكنولوجيا الحديثة في ارتكاب الجريمة، لاسيما إن كان الجاني يعمل في شركة معينة تعتمد على الحاسب الآلي في عملها، فيكون لديه المعلومات اللازمة كافة لتحقيق اختراقات متعددة ومتتالية لأنظمة الحاسب الآلي في الشركة؛ فتحقق أرباحًا طائلة، وما يثب ذلك الواقع الذي نعيشه[3].

2- جريمة عابرة للحدود:

أعطى انتشار الإنترنت إمكانية لربط العالم في زاوية واحدة من خلال أجهزة الحاسوب المرتبطة بالشبكة العنكبوتية، وكذلك ارتباط أجهزة الهاتف النقال بشبكة الإنترنت، وهذا ما يجعل جريمة الحاسوب أو الهاتف النقال عابرة للحدود، وبالتالي قد يكون الجاني في دولة، والمجني عليه في دولة أخرى[4]، وهذا

---

[1]. ثنيان ناصر آل ثنيان، إثبات الجريمة الإلكترونية دراسة تأصيلية تطبيقية، رسالة مقدمة لاستكمال متطلبات درجة الماجستير في السياسة الجنائية، جامعة نايف للعلوم الأمنية، الرياض، 2012م، ص22.

[2]. المرجع نفسه.

[3]. ثنيان ناصر آل ثنيان، المرجع السابق، ص23.

[4]. عبد الله دغش العجمي، المشكلات العلمية والقانونية للجرائم الإلكترونية دراسة مقارنة، رسالة مقدمة لاستكمال متطلبات الماجستير، جامعة الشرق الأوسط، 2014م، ص20.

الأمر يتطلب وجود تنظيم قانوني دولي يعمل على حماية المجني عليه من الانتهاكات التي قد يتعرض لها من قِبل أشخاص يقيمون في دولة أخرى؛ فجرائم الحاسوب لم تُعد تقتصر على إقليم فلا تتعداه، بل أصبح بالإمكان ارتكاب جريمة عن طريق الحاسوب باختراقه لحاسوب في قارة أخرى، وقد أدى هذا التشتت إلى ضعف إمكانية مواجهة الجريمة الإلكترونية، وتُعد ملاحقة المجرمين فيها من النوع العسير؛ لاختلاف الإجراءات الجنائية من بلد إلى آخر، أو النزاع حول القانون الواجب تطبيقه[1].

3- صعوبة مكافحة الجريمة الإلكترونية:

تُعد الجريمة الإلكترونية جريمة مخفية بحيث لا يستطيع الشخص أو الشركة اكتشافها إلا بعد حصولها في بعض الأحيان؛ وذلك لأنها جريمة صامتة تحدث عن بُعد، ومما يُصعِب مكافحة الجريمة – أيضًا– مساهمة المجني عليه في إخفائها حفاظًا على سمعة الشركة، وغالبًا ما يتجه المجني عليه نحو اتخاذ إجراءات داخلية دون إبلاغ السلطات المختصة في ذلك الأمر، ويأتي إحجام المجني عليه من الإبلاغ عن الجريمة في كثير من المؤسسات الادخارية والبنوك؛ لأن مجلس إدارتها يرى بأن المطالبة القضائية سوف تؤثر على ثقة العملاء في البنك أو المؤسسة[2]، ويرى الباحث بأن إحجام الشركات والمؤسسات عن الإبلاغ عن الجرائم الإلكترونية يشجع المجرم على ارتكاب الجريمة؛ لأنه أمِن العقوبة، كذلك يؤدي إلى ضعف مكافحة الدولة للجرائم الإلكترونية؛ لعدم تلقيها الشكاوى من الجهات المتضررة، ونرى بأن هذه الجرائم بحق البنوك وبعض المؤسسات تضر بالمصلحة العامة، وبالتالي يحق للدولة التدخل لمكافحتها حتى دون أي بلاغ أو شكوى من الجهة المتضررة من الجريمة.

ثالثًا: أنواع الجرائم الإلكترونية

يمتلك المجرمون سمات مشتركة يمكن إجمالها في شخص واحد يمتلك الخبرة والمهارة في القرصنة على أجهزة الحاسوب أو أجهزة الهاتف النقال، فالمجرم المحترف هو الذي يستخدم التقنية الحديثة من أجل ممارسة عملية النصب والاحتيال والاعتداء والسرقة وغيرها؛ بغية الحصول على المال[3]، ومن خلال ذلك يتضح لنا أن هناك أنواعًا للجرائم الإلكترونية متعددة كالآتي:

---

[1] الجرائم الإلكترونية، معهد الكويت للدراسات القضائية والقانونية، مرجع سابق، ص14.

[2] جلال الدين محمد صالح، المرجع السابق، ص25.

[3] الملتقى الوطني، آليات مكافحة الجريمة الإلكترونية في التشريع الجزائري، الجزائر، 2017م، ص10 وما بعده

1-الجرائم الماسة بالأشخاص:

هذه الجرائم تتم عبر المس بشخصية المجني عليه، وتسمى بجرائم الإنترنت الشخصية، مثل: جريمة سرقة الهوية، أو سرقة الاشتراك في موقع شبكات الإنترنت[1]، كذلك تتم من خلال الوصول إلى المعلومات بشكل غير شرعي كسرقة المعلومات الشخصية للأفراد، أو الاطلاع عليها، أو حذفها، أو تغييرها بما يحقق هدف المجرم، وأكثر ما يتعرض له الأشخاص هو الاعتداء على حرمة المراسلات الخاصة التي تتعدد بالفتح والإخفاء أو الاختلاس أو التعدي أو إفشاء الأسرار، ومن أقوى الوسائل التي يتبعها منفذ الجريمة الإلكترونية هي الاتخاذ من رسائل البريد الإلكتروني فرصة للإيقاع بالضحايا والتي يتم إرسال الملايين منها يوميًا شأنها شأن بقية وسائل التواصل الأخرى، ومن أشهر الجرائم المرتبطة بالبريد الإلكتروني هي جرائم الغش وإرسال الفيروسات والتهكير والتشهير[2] وغيرها من الجرائم التي يُهاجم بها الأشخاص.

2-جرائم انتهاك المُلكية:

هذه الجريمة تشكل خطورة على المؤسسات والهيئات الخاصة كالبنوك والشركات والأجهزة الحكومية، وتتمثل الجريمة بقيام المجرم بإرسال برامج ضارة لتدمير الأجهزة الخاصة بالمؤسسات، وغالبًا ما تتصف هذه الهجمات بالسياسية البحتة التي قد تحدث بين الدول، وتُعد جرائم الإضرار بالبيانات من أخطر الجرائم التي تؤثر على المؤسسات، وتشمل كل أنشطة تعديل أو محو أو سرقة أو إتلاف البيانات، وبالنسبة لتلك الجرائم التي يرتكبها أفراد أو محترفون يطلق عليهم: المحترفون ذوو القبعات السوداء، وهم يقومون بذلك بغرض الاستفادة المالية، وقد تكبدت المؤسسات في الولايات المتحدة الأمريكية خلال العام 2003م، خسارة مالية كبيرة فاقت: (70 مليون دولار أمريكي؛ جراء تعطيل نشاط نظم المعلومات في أمريكا[3].

رابعاً: الجرائم الماسة بالمجتمع

تُعد هذه الجرائم ماسة بحق الأشخاص والمؤسسات بأنواعها، ويهدف المجرمون من وراء ذلك إلى جني الأموال الطائلة من خلال الابتزاز الذي يمارس على الأشخاص أو المؤسسات، غير أن جرائم الابتزاز الواقعة على الأشخاص تمتد إلى التأثير على أمن المجتمع خاصة في المجتمعات القبلية التي ترى أن العار لا يمكن أن يكون الانتقام له إلا من خلال الدم، وتأتي الخطورة الكبرى حين يتم استخدام هذه الجرائم ضد المؤسسات المالية أو شركات عملاقة كبرى؛ فتسبب لها أضرارًا كبيرة، كذلك عندما تهاجم أنظمة

---

[1]. المرجع نفسه، ص10.

[2]. عبد الحليم موسى يعقوب، الإعلام الجديد والجريمة الإلكترونية، الدار العالمية للنشر، السعودية، 2014م، ص223.

[3]. عبد الحليم موسى يعقوب، المرجع السابق ، ص221.

حكومية، وتخلف أضرارًا بالغة في الاقتصاد القومي لبعض الدول، أو ممارسة التجسس الصناعي والعسكري والتخريب المعلوماتي الذي ينعكس أثره على المجتمع[1]، وتُعد جرائم تزوير البيانات من أكثر الجرائم شيوعًا من بين الجرائم الإلكترونية، ويكون ذلك بالدخول إلى قاعدة البيانات الموجودة، وتعديل تلك البيانات من حيث الإلغاء أو الإضافة[2]، كما يمكن للتنظيمات الإرهابية أو الدول الاستعمارية أن تمارس أبشع الجرائم بحق المجتمع من خلال استخدام التقنيات الحديثة في صنع المتفجرات وتفجيرها عن بُعد، أو تحديد الأهداف من قبل دولة الاحتلال لقصف الأبرياء بطريقة همجية، وتُعد الأجهزة الإلكترونية سلاحًا ذا حدين يمكن استخدامها لخدمة المجتمع أو ضده.

المطلب الثاني:

دور الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية وموقف التشريعات القانونية العربية منها

مع التقدم التكنولوجي الحاصل تُعد الجريمة الإلكترونية خارقة للعادة الكونية، إذ من خلالها يمكن للأشخاص ممارسة الجرائم بحق الأشخاص الآخرين والمؤسسات بطريقة احترافية دون أن يتنبه المستهدفون لذلك، لكن تقدم الذكاء الاصطناعي كان أسرع في مكافحة الجرائم الإلكترونية من حيث اكتشافها منذ اللحظة الأولى، وتُعد التشريعات العربية منقسمة في مجال مكافحة الجرائم الإلكترونية، فمنها ما تُعد قديمة لم تتناول الجرائم الإلكترونية بقانون منفصل، ولا تزال تستخدم طرائق تقليدية في مواجهة الجريمة الإلكترونية، ومنها ما تناول ذلك بقانون، ورتب لها جزاء معينًا، واستخدمت تكنولوجيا الذكاء الاصطناعي في مواجهة الجرائم الإلكترونية، وسنتعرف في الفرعين الآتيين على دور الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية وموقف الأنظمة العربية منها.

الفرع الأول:

دور الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية

بما أن الجرائم الإلكترونية ذات طابع تقني حديث؛ حيث تُعد جرائم مخفية وغير قابلة للتكشف بسهولة، فإن الذكاء الاصطناعي ذا طبيعة خاصة في مكافحة الجريمة الإلكترونية من خلال المراقبة الرقمية عبر الأجهزة الذكية، كما أن تكامل الذكاء الاصطناعي في تنقيب البيانات والشبكات العصبية الذكية يساعد في تحليل البيانات المخزنة وتدعيمها لإدارة أمن المعلومات، واكتشاف شبكات التجسس والتلاعب بالبيانات،

---

[1]. لطرش فيروز ابن عزوز حاتم، المرجع السابق، ص325.

[2]. دولي لخضر ناصري نفيسة، دور الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية، مجلة المؤشر للدراسات الاقتصادية، المجلد 2،العدد2، 2018م، ص 59.

ويُعد الهدف من استخدام الذكاء الاصطناعي هو تطوير وتحسين العمليات الرقابية، وتحسين إنشاء القواعد المعرفية بخصوص التهديدات والمخاطر المتعلقة بأمن المعلومات[1]؛ مما يساعد على كشف الجريمة الإلكترونية في وقت مبكر أو التنبؤ بها قبل وقوعها.

أولًا: دور الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية التي تقع على الأموال

تُعد الجرائم على الأموال من أكبر العوائد التي تعود على مجرمي الجرائم الإلكترونية بالنفع الكبير، وغالبًا ما يستخدم المجرمون أسلوب القرصنة والابتزاز من أجل الحصول على الأموال، وبالتالي فإن العالم يحتاج إلى جدار حماية يحول بينه وبين مرتكبي هذه الجرائم، ولما للذكاء الاصطناعي من دور مهم في مكافحة الجريمة كان لا بُد من دمج أجهزة الذكاء الاصطناعي في الأنظمة المالية المحاسبية وتفعيل الشبكات العصبوية والخوارزميات التي تستخدم في التنبؤ بالجريمة قبل وقوعها؛ حيث تعمل الخوارزميات في العديد من مصادر البيانات الضخمة؛ إذ تُعد هي الوسيلة التي تستخدم لمسح وتصفية وفهم وتحليل البيانات وفرزها، وتساعد على اكتشاف الجرائم قبل حدوثها في وقت كافٍ للشركات المالية وأصحاب الأموال لاتخاذ الإجراءات اللازمة[2]، وتستطيع الدولة استخدام تقنيات الذكاء الاصطناعي لمجابهة الجريمة الإلكترونية، وتحسين عملها؛ لخلق نوع من التوازن بين الجرائم المرتكبة ووسائل مجابهتها، حيث يعمل الذكاء الاصطناعي على مواجهة الجريمة وفقًا للآلية والتقنية المحددة له؛ حيث يقوم بترتيب العمل الأمني ومعالجة البيانات والتقصي عنها في العالم الرقمي وأنظمة المعلومات[3].

ثانيًا: الشرطة الرقمية

وتعني تطوير أجهزة الشرطة من خلال استخدام تقنيات الذكاء الاصطناعي لتصبح أكثر اعتماداً على الأجهزة الحديثة[4]، وربط كافة الأنظمة التابعة للشركات والمؤسسات الخاصة تحت رقابة الدولة، وبالتالي فإن أي جريمة قد تحدث تستطيع الشرطة التنبؤ بها ومكافحتها قبل وقوعها[5]، كما يساهم الذكاء الاصطناعي

---

[1]. دولي الخضر، المرجع السابق، ص60.

[2]. رانا مصباح عبد المحسن عبد الرزاق، المرجع السابق ص17.

[3]. الأخنش نورة أمينة، العيداني محمد، المرجع السابق، ص537

[4]. حمزة قده، إيمان كحيط، توظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية، المؤتمر الدولي العام حول التكنولوجيا الرقمية من التأصيل إلى الابتكار، دون مجلد، الإمارات العربية المتحدة، جامعة أم القيوين، 2022، ص8.

[5]. البابلي عمار ياسر محمد زهير، المرجع السابق، ص151.

الشرطة الرقمية في مجال التحقيق الرقمي الذي يسارع في اكتشاف هوية الجاني من خلال الرسائل الخاصة به أو الرقم الهاتفي الخاص به، والكشف عن الأدلة، وتحليل البيانات الخاصة بالمجرمين، وجعلهم تحت المراقبة، وتعتمد الدول المتقدمة على بصمة المخ التي تستخدم في مسح دماغ المشتبه به قبل التحقيق الجنائي، والتي من خلالها يتم تحديد ما إذا كان المجرم لديه معلومات معينة عن الجريمة المطلوبة أم لا[1]، وبالتالي لا يستطيع المجرم الكذب أو استخدام طرائق احتيالية في التزييف على الشرطة الرقمية، وتختلف تقنية بصمة المخ عن جهاز كشف الكذب الذي يأتي من خلال استخدام الضغط العصبي؛ حيث إن الشخص الذي يكذب يزداد قلقه فضلًا عن التغيرات العاطفية التي تحصل للمجرم، أما بصمة المخ فيكمن من خلالها كشف الكذب دون الحاجة إلى الضغط العصبي[2]، كما يُعد جهاز الإنذار المبكر صمامًا للمحافظة على الأمن والاستقرار؛ حيث يشكل الإنذار المبكر أحد المكونات التي تساهم في توقع حدوث الجريمة والمنع الوقائي منها[3].

ثالثًا: مكافحة جرائم الإرهاب السيبراني

يُعد الإرهاب السيبراني من أكثر الظواهر الإجرامية مدعاة للقلق خاصة في السنوات الأخيرة لاسيما مع انتشار البرامج الذكية والخبيثة لأجهزة الحاسوب؛ إذ يستخدم الإرهابيون شبكة الإنترنت في وضع شبكة قنابل إلكترونية مؤقتة في عدد من المدن، ويمكن ربطها بعضها ببعض وتفجيرها في وقت واحد، وليس بالضرورة أن يتواجد المجرم في الدولة نفسها، وهذه الجرائم قد تتسبب في تعطيل الشركات التجارية، مثل: شركات الطيران والبورصات والبنوك وتغير مستويات الاحتياط لدى البنوك[4]، ويبرز دور الذكاء الاصطناعي في مكافحة الإرهاب السيبراني من خلال المصادر التقنية التي تعتمد على شبكات التتبع كالتصوير بالأقمار الاصطناعية، وتتبع البيانات المستمدة من الهواتف المحمولة لتحديد الموقع الجغرافي للمجرم، ويمكن استخدام كاميرات (آي بي، ونشرها في جميع الأماكن المهمة والحيوية لضبط مراقبة البث المباشر للأنشطة غير القانونية التي تقوم الكاميرات بمراقبتها، وما يميز هذه الكاميرات هو نظام التعرف على الوجه الذي يطابق أوجه الأشخاص الذين أمام الكاميرات بالأشخاص المدرجين لدى القائمة السوداء

---

[1]. رانا مصباح عبد المحسن عبد الرزاق، المرجع السابق، ص18.

[2]. المرجع نفسه، ص18.

[3]. سعود عبد القادر الشاعر، المرجع السابق ص21.

[4]. علي أحمد إبراهيم، تطبيقات الذكاء الاصطناعي في مواجهة الجرائم الإلكترونية، المجلة القانونية، دون عدد، دون سنة نشر، ص22-28.

المخزنة مسبقًا لدى الأجهزة الأمنية، كما تساعد تقنيات الذكاء الاصطناعي على خلق بيئة عمل قابلة لظاهرة التنبؤ بالجرائم قبل وقوعها من خلال عمليات تحليل البيانات بطريقة معقدة[1].

وللذكاء الاصطناعي أثر كبير في المجال الأمني من خلال توفير الحماية اللازمة لرجال الأمن في عمليات مواجهة الإرهاب السيبراني؛ حيث يتم استخدام البرامج الإلكترونية على الحاسب الآلي لتحقيق عملية رصد وتتبع المجرمين، وكذا نظام المراقبة الحية والذكية، ونظم الاستلام الإلكتروني[2].

رابعًا: دور الذكاء الاصطناعي في تطوير الأجهزة الأمنية

ظلت أجهزة الأمنية–لاسيما في الدول الفقيرة– تعمل بالنظام التقليدي لمكافحة الجريمة، ومع التقدم التكنولوجي في العالم لم تُعد الوسائل البدائية مجدية في مكافحة الجريمة؛ إذ أصبحت معقدة ومركبة، وبإمكان المجرم أن يقوم بها عن بُعد من خلال الأجهزة الإلكترونية، وقد ساهم الذكاء الاصطناعي في تعزيز وتطوير المؤسسات الأمنية بشكل غير مسبوق، فقد وفر للجهات الأمنية فرصة التنقيب عن ملايين المعلومات الموجودة في مواقع التواصل الاجتماعي وكاميرات المراقبة في الشوارع ووسائل الإعلام والبيانات الحكومية للعثور على أية معلومة تتصل بمرتكبي الجرائم[3]، وتستخدم بعض المؤسسات الأمنية مثل الولايات المتحدة الأمريكية أجهزة محاكاة أبراج الهواتف الخلوية المعروفة باسم "ستينجراي"، وهي عبارة عن أجهزة رصد وتجسس محمولة تقوم بإطلاق تردد يفوق تردد الاتصالات الخلوية الحقيقية القريبة منها، وهو ما يدفع الأجهزة المحمولة بالاتصال بستينجراي، مما يجعل الجهاز يطلع على قواعد البيانات والرسائل والاتصالات في منطقة بأكملها، كما يمكن استخدام الذكاء الاصطناعي من قِبل قوات حفظ السلام الدولية التي تعمل على تخفيف حدة التوتر بين الأطراف المتنازعة، والتقليل من الخسائر البشرية عن طريق التنبؤ بأماكن الغارات الجوية، وتنبيه المدنيين في المناطق المستهدفة[4].

---

[1]. سعود عبد القادر الشاعر، المرجع السابق، ص17.

[2]. عمار ياسر زهير البابلي، المرجع السابق، ص136.

[3]. المرجع نفسه، ص149 وما بعده

[4].على شريف، دور الذكاء الاصطناعي في نشر وتعزيز ثقافة السلام في مناطق النزاعات المسلحة، 2021م، ص4.

الفرع الثاني:

موقف الأنظمة العربية من الذكاء الاصطناعي

مع تقدم التكنولوجيا في العالم والتطور الحاصل في ارتكاب الجرائم عن طريق استخدام التقدم العلمي كان لا بُد للقوانين أن تسلك مسلكًا يوازي التقدم والتطور المستخدم في ارتكاب الجريمة، فكان لا بُد من وجود تشريعات تنظم عملية مكافحة الجريمة الإلكترونية والإرهاب الإلكتروني؛ وتقنيات حديثة تستخدمها الدول لمجابهة الجرائم الإلكترونية، لذلك عملت بعض الدول العربية على تحديث تشريعات تواكب التطور والتقدم التكنولوجي وعملت على استخدام وسائل الذكاء الاصطناعي في مكافحة الجريمة، والبعض الآخر أدخل تعديلات على القوانين تشمل جزئية تشير إلى مكافحة الجرائم الإلكترونية وما زال يستخدم طرق تقليدية لمكافحة الجريمة الإلكترونية، ومن هنا سوف نتعرف في هذا الفرع على موقف بعض أنظمة الدول العربية في مكافحة الجريمة الإلكترونية عبر استخدام الذكاء الاصطناعي على النحو الآتي:

أولًا: موقف المشرع السعودي

تمثل الجريمة الإلكترونية مصدر خطر يهدد الجميع؛ فقد عرفها نظام مكافحة الجرائم المعلوماتية في السعودية أنها: "أي فعل يُرتكب متضمنًا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام"[1]، ويمثل الذكاء الصناعي بالنسبة للمملكة العربية السعودية ضرورة ملحة لاعتماد قطاعات عدة عليه، مثل: التعليم والصحة والمؤسسات الأمنية والعسكرية[2]؛ فقد صدر نظام مكافحة الجرائم المعلوماتية بموجب المرسوم الملكي رقم (17 لسنة 2010م، تضمن هذا المرسوم صورًا لجرائم المعلومات بشكل عام وجرائم الإرهاب الإلكتروني بشكل خاص، وقد استخدم النظام السعودي وسائل الذكاء الاصطناعي في سبيل منع الجرائم الإرهابية بالذات من خلال تجريمه إنشاء مواقع إلكترونية للمنظمات الإرهابية؛ لتسهيل عملية التواصل بين قياداتها، وقد غرم أي شخص يسعى لذلك بغرامة تبلغ خمسة ملايين ريال سعودي مع السجن عشر سنوات، وتستخدم السعودية تقنيات عالية في سبيل توحيد الجهود الأمنية لمكافحة الجريمة عبر الذكاء الاصطناعي[3]، كما أنها تستخدم أعمال الشرطة الرقمية وكاميرات المراقبة الحديثة التي تحدد هوية المجرمين، وترسل إشارتها إلى الشرطة للقبض عليهم، وقد عمل المشرع السعودي على تدريب فريق خاص من الشرطة في مجال التقنيات الحديثة سواء في مجال مكافحة الجريمة الإلكترونية قبل وقوعها أو

---

[1]. مادة (1) الفقرة (8) من نظام مكافحة الجرائم المعلوماتية السعودي، أقره المجلس الوزاري في 1428هـ-2007م.

[2]. الذكاء الاصطناعي، مركز البحوث، دبي، 2021م، ص6.

[3]. رانا مصباح عبد المحسن عبد الرزاق، المرجع السابق، ص23.

من خلال إثبات الجريمة بعد وقوعها، وقد أتاح للشرطة استخدام التقنيات العالية للوصول إلى أدلة الإثبات[1]، وقد أطلقت السعودية العديد من المنصات والهيئات التي تستخدم الذكاء الاصطناعي لمكافحة الجرائم الإلكترونية مثل منصة "فوكال" لمكافحة الجرائم المالية عبر الذكاء الاصطناعي[2]، وعملت السعودية على تأسيس الهيئة الوطنية للأمن السيبراني للحد من الجرائم الإلكترونية، كما عملت على تعزيز وتشجيع التعاون العربي والدولي في مجال مكافحة الجرائم الإلكترونية من خلال مشاركتها في المبادرات الدولية وتبادل المعلومات والخبرات في مجال الأمن السيبراني[3].

ثانيًا: موقف المشرع الفلسطيني

يعاني القانون الفلسطيني انشطاراً بين الضفة الغربية من جهة وقطاع غزة من جهة أخرى، حيث يطبق القانون رقم (74 لسنة 1936م، في غزة، والقانون رقم (16 لسنة 1960م في الضفة الغربية، لكن هذه القوانين لم تتطرق لمكافحة الجرائم الإلكترونية، وبالتالي تم تعديل القانون في الضفة الغربية في العام 2010م، وأفرد المشرع عقوبات خاصة لكل من استخدم الأجهزة الإلكترونية بقصد الإساءة للغير أو التنصت عليهم أو انتهاك خصوصياتهم[4]، ولم تكن القوانين المشار إليها تعاقب على الجريمة الإلكترونية، ونتيجة الانقسام السياسي الحاصل اتجهت قطاع غزة إلى سد الفراغ من خلال تعديل بعض مواد قانون العقوبات الساري في القطاع، وأضافت المادة (262 مكرر والتي جاء فيها: "كل من أساء عمدًا لاستعمال أجهزة الخطوط الهاتفية أو الإنترنت أو أي وسيلة تكنولوجية أخرى، بأن روج أو نقل أو طبع أو نسخ مواد إباحية أو إزعاج الغير أو وجه إليهم ألفاظًا بذيئة أو مخلة في الحياء..."، من خلال ذلك اتجه المشرع في غزة إلى تعديل قانون العقوبات؛ من أجل إرساء مبدأ الشرعية في فرض العقوبات بالجرائم الإلكترونية، كذلك أدخل تعديلات في عام 2010م، على المواد (545، 547، 548 وما بعدها حيث تم إفراد باب خاص بجرائم المعلومات، لكن استخدام الذكاء الاصطناعي في مجال مكافحة الجريمة بما فيها مقاومة

---

[1]. ثنيان ناصر آل ثنيان، إثبات الجريمة الإلكترونية: دراسة تأصيلية تطبيقية، رسالة مقدمة لاستكمال متطلبات درجة الماجستير في السياسة الجنائية، جامعة نايف للعلوم الأمنية، الرياض، 2012م، ص45 وما بعده

[2]. نسيم رمضان، صحيفة الشرق الأوسط العرب الأولى، تاريخ الزيارة 2024/4/11م، وقت الزيارة 10 مساءً على الرابط: https://aawsat.com

[3]. رانا مصباح عبد المحسن، آليات مكافحة الجريمة الإلكترونية في السعودية "دراسة تحليليه"، المجلة القانونية، دون مجلد، دون عدد، 2022م، ص13.

[4]. إيمان يوسف صبرة، المرجع السابق، ص30.

الاحتلال كان لافتًا في ظل الحصار التي تشهده غزة منذ عشرات السنوات؛ إلا أنها كانت تستخدم وسائل وتقنية حديثة استطاعت من خلالها تحقيق مكاسب كبرى في مكافحة الجرائم الإلكترونية، ويتضح من التعديلات المنصوص عليها في قانون العقوبات الفلسطيني المعدل من المادة (546 إلى المادة (560 والتي تناولت الجرائم الإلكترونية، أن المشرع الفلسطيني قد تناول أغلب صور الجرائم الإلكترونية التي ظهرت على الساحة الفلسطينية[1]، ولكنها لم تكن شاملة لجميع الجرائم الموجودة في فلسطين، لكن المشرع الفلسطيني تدارك الموقف في التعديل الحاصل على قانون العقوبات وأضاف جرائم لم يكن يعاقب عليها القانون من قبل، وبالتالي لا يستطيع المجرم الإلكتروني الإفلات من العقاب[2]، ويتضح من ذلك بأن المشرع الفلسطيني يتخذ طرقًا وتقنيات حديثة في مكافحة الجرائم الإلكترونية ولكنها لا ترقى الى مستوى تقنية الذكاء الاصطناعي في مكافحة الجريمة.

ثالثًا: موقف المشرع الإماراتي

تسعى دولة الإمارات إلى عملية دمج تقنيات الذكاء الاصطناعي في العمل الجنائي من خلال التنبؤ بالجرائم بطريقة ذكية، وتعمل على إدخال الذكاء الاصطناعي في مجال عمل الأدلة الجنائية وعمليات الشرطة، إلى جانب استخدامه في تعزيز الأمن والسلامة في الطرقات، واستخدامه لإدارة الكوارث والأزمات كنظام الأزمات والحشود، وهو نظام ذكي يعمل على دراسة وتحليل الحشود ورفع تقرير مباشر إلى متخذي القرار[3]، وتسعى دولة الإمارات إلى الاعتماد الكلي على تقنيات الذكاء الاصطناعي بشكل كلي بحلول العام 2031م، وتتبنى دولة الإمارات أحدث التقنية في الأداء المعلوماتي لخلق البيئة المتميزة على مستوى العالم[4]، وتعمل أيضاً على تطوير أنظمة الذكاء الاصطناعي بشكل كبير في مجال مكافحة جرائم القرصنة الإلكترونية أو الجرائم العادية، ومن الآليات التي انتهجت في دولة الإمارات تنمية وتطوير الكفاءات العلمية المتخصصة والقدرات المحلية في مجال الذكاء الاصطناعي، وتدريب موظفيها عبر دورات متخصصة في علم البيانات، وخلق ثقافة الذكاء الاصطناعي لدى المجتمع، وتعمل كذلك على إدماج الجهات الحكومية كافة في مجال مكافحة الجريمة الإلكترونية من خلال تضافر الجهود الإعلامية، وقد خصصت لذلك وزارة

---

[1]. إيمان يوسف صبرة، المرجع السابق، ص 27 وما بعده

[2]. المرجع نفسه.

[3]. سعود عبد القادر الشاعر، المرجع السابق، ص19.

[4]. رانا عبد الرزاق المصباح، المرجع السابق، ص18.

مستقلة في حلول العام 2017م[1]، وقد أصدرت دولة الإمارات العربية المتحدة قانون مكافحة الجرائم المعلوماتية رقم (2 لسنة 2006م، الذي تم تعديله في عام 2012م، وهنا يرى الباحث بأن دولة الإمارات قد اتجهت نحو التقدم في استخدام الذكاء الاصطناعي لمكافحة الجرائم الإلكترونية.

رابعًا: موقف المشرع اليمني

ما زال المشرع اليمني يعمل بالطرق التقليدية لمكافحة الجرائم الإلكترونية على الصعيدين العملي والتشريعي؛ إذ لا يوجد قانون خاص بتنظيم أحكام الجرائم الإلكترونية في اليمن، فقد أشار الدستور اليمني في المادة (53 منه إلى أن "حرية وسرية المواصلات البريدية والهاتفية والبرقية وكافة وسائل الاتصال مكفولة، ولا يجوز مراقبتها ..."[2]، وقد أكد على ذلك قانون الإجراءات الجزائية اليمني[3]، وقد حدد لها قانون العقوبات اليمني الجزاء المترتب على ذلك في عدة نصوص قانونية، نذكر منها نص المادة (255 التي نصت على أنه "يعاقب بالحبس مدة لا تزيد على سنة أو بغرامة من فتح بغير حق خطابًا مرسلًا للغير، أو احتجز رسالة برقية أو هاتفية... "[4]، ومع هذا ما زالت اليمن تعمل بالطرق التقليدية للبحث والتحري عن الجرائم الإلكترونية في مجال مكافحتها عن طريق الشرطة العادية، ولا تمتلك الأجهزة الأمنية–خاصة بعد الحرب– أي مقومات إلكترونية تستخدم لمكافحة الإرهاب الإلكتروني في اليمن؛ ويعود ذلك إلى عدة أسباب، منها: هشاشة الدولة وتمزقها في الفترات الأخيرة، لكن الملاحظ أن الجرائم الإلكترونية انتشرت بشكل لافت خاصة جرائم الابتزاز الإلكتروني لدى الشباب والشابات، وذلك من خلال القيام باختراق أجهزة الهاتف المحمول، وسحب بيانات وصور خاصة للمجني عليه وابتزازه بها، وعند تعامل الشرطة مع هكذا قضايا تصبح الإجراءات أكثر صعوبة، ولا تستطيع الشرطة متابعة المجرم في عدة حالات، ولم تدخل أجهزة الذكاء الاصطناعي في اليمن الخدمة للأسباب المشار إليها سابقًا.

---

[1]. سعود عبد القادر الشاعر، المرجع السابق، ص22.

[2]. المادة (53) من الدستور اليمني.

[3]. تنص الفقرة (2) من المادة (12) من قانون الإجراءات الجزائية اليمني على أن "حرية المراسلات البريدية والسلكية واللاسلكية وكافة وسائل الاتصال مكفولة وفقًا للدستور ...".

[4]. المادة (255) من قانون العقوبات اليمني.

الخاتمة:

تناولت هذه الدراسة دور الذكاء الاصطناعي في مواجهة الجريمة الإلكترونية، وموقف الأنظمة العربية من تحديث القوانين لمواكبة التقدم التكنولوجي، واستخدام الذكاء الاصطناعي في مواجهة الجرائم الإلكترونية، وقد توصلت الدراسة إلى مجموعة من النتائج والتوصيات كالآتي:

أولاً: النتائج

1. أكدت الدراسة على دور استخدام الذكاء الاصطناعي في مواجهة الجرائم الإلكترونية قبل حدوثها، أو المساعدة في التوصل لإثبات الجريمة والكشف عن هوية المجرمين بعد حدوث الجريمة.
2. بينت الدراسة خطورة الجرائم الإلكترونية على مستوى الأفراد أو المجتمع أو الدول من خلال قيام المجرمين باستخدام هذه الجرائم لجني الأموال من المؤسسات المتضررة من جرائمها؛ كونها جرائم عابرة للقارات، ويصعب كشفها أو التنبؤ بها بسهولة.
3. كشفت الدراسة عن إمكانية استخدام التقنيات الصناعية في مواجهة جرائم المحتلين للبلدان، وإمكانية إرباك التقنيات الاصطناعية التي يعتمد عليها العدو في جرائمه ضد الشعوب.
4. بينت الدراسة موقف بعض الأنظمة العربية من مواكبة التقدم التكنولوجي، واستخدام وسائل الذكاء الاصطناعي من أجل مكافحة الجريمة؛ حيث عمل النظامان السعودي والإماراتي على مواكبة التقدم الاصطناعي بشقيه الصناعي والقانوني؛ فقد أعدت قوانين مستقلة لمواجهة الجرائم الإلكترونية، وعملت على تطوير أداء الأجهزة الأمنية من حيث تمكينها من استخدام وسائل الذكاء الاصطناعي للكشف عن الجرائم الإلكترونية، بينما ذهب المشرع الفلسطيني في غزة إلى تعديل قانون العقوبات لفرض مبدأ الشرعية في مكافحة الجرائم الإلكترونية، وما يزال المشرع اليمني يستخدم القوانين القديمة التي أشارت إلى مواجهة الجرائم الإلكترونية بشكل خفيف، وما زالت الطرق البدائية هي السبيل الوحيد لمكافحة الجرائم الإلكترونية.
5. بينت الدراسة إمكانية استخدام الشبكات العصبوية والخوارزميات لمواجهة الجرائم الإلكترونية من حيث استخدام قواعد البيانات وتحليلها؛ لكشف هوية المجرمين، والمساعدة في كشف كذبهم في التحقيق باستخدام الذكاء الاصطناعي.

ثانياً: التوصيات

1. يوصي الباحث، المشرعين اليمني والفلسطيني بضرورة إصدار قانون ينظم عمل مكافحة الجرائم الإلكترونية والعقوبات المناسبة لها، وبناء جهاز أمني مدرب لاستخدام تقنيات الذكاء الاصطناعي، وتوفير الأجهزة الخاصة به.
2. تعزيز التعاون العربي والدولي وتبادل المعلومات والخبرات بين الدول والمنظمات الدولية المختصة في مجال مكافحة الجرائم الإلكترونية، وذلك للتصدي للتهديدات السيبرانية المتزايدة والمبتكرة عبر تقنيات الذكاء الاصطناعي.
3. يوصي الباحث بضرورة استخدام أجهزة الذكاء الاصطناعي لمواجهة الجرائم الإلكترونية؛ لثبوت فعاليتها بكفاءة عالية في قمع أغلب الجرائم المتعلقة بالإرهاب السيبراني.

بيان تضارب المصالح:

يقر جميع المؤلفين أنه ليس لديهم أي تضارب في المصالح.

قائمة المصادر والمراجع

أولًا: الكتب العامة

1. أروى بنت عبد الرحمن الجلعود، أحكام تطبيقات الذكاء الاصطناعي في القضاء، السعودية، الطبعة الأولى، 1444هـ.
2. سعود عبد القادر الشاعر، دور الذكاء الاصطناعي في تفعيل إجراءات التحقيق الجنائي في الجرائم الإلكترونية (دراسة مقارنة، جامعة عجمان، الإمارات العربية المتحدة، 2020م.

ثانيًا: الرسائل العلمية

1. إيمان يوسف صبرة، حقوق المجني عليه في الجرائم الإلكترونية في التشريع الفلسطيني: دراسة مقارنة مع القانون والشريعة الإسلامية، رسالة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير، الجامعة الإسلامية بغزة، فلسطين، 2020م.
2. ثنيان ناصر آل ثنيان، إثبات الجريمة الإلكترونية: دراسة تأصيلية تطبيقية، رسالة مقدمة لاستكمال متطلبات درجة الماجستير في السياسة الجنائية، جامعة نايف للعلوم الأمنية، الرياض، 2012م.
3. جلال الدين محمد صالح، إثبات الجريمة الإلكترونية: دراسة تأصيلية تطبيقية، رسالة مقدمة لاستكمال متطلبات درجة الماجستير في السياسة الجنائية، جامعة نايف للعلوم الأمنية، الرياض، 2012م.
4. رشا محمد صائم، تطبيقات الذكاء الاصطناعي في اتخاذ القرارات الادارية، رسالة مقدمة لاستكمال متطلبات درجة الماجستير، جامعة الشرق الأوسط، 2022م.
5. عبد الله دغش العجمي، المشكلات العلمية والقانونية للجرائم الإلكترونية: دراسة مقارنة، رسالة مقدمة لاستكمال متطلبات الماجستير، جامعة الشرق الأوسط، 2014م.

ثالثًا: المجلات والدوريات العلمية

1. الأخنش نورة أمينة، العيداني محمد، الذكاء الاصطناعي كآلية لمجابهة الجريمة الإلكترونية، مجلة القانون والعلوم البيئية، المجلد2، العدد2، 2023م.
2. دولي لخضر، ناصري نفيسة، دور الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية، مجلة المؤشر للدراسات الاقتصادية، المجلد 2، العدد 2، 2018م.
3. رانا مصباح عبد المحسن عبد الرزاق، دور الذكاء الاصطناعي في مواجهة جرائم الإرهاب الإلكتروني: دراسة مقارنة، المجلة الأكاديمية لجامعة نورة، الرياض، 2023م.

4. رانا مصباح عبد المحسن، آليات مكافحة الجريمة الإلكترونية في السعودية "دراسة تحليليه" المجلة القانونية، دون مجلد، دون عدد، 2022.
5. سميرة معاشي، ماهية الجريمة المعلوماتية، مجلة المنتدى القانوني، جامعة محمد خضير بسكرة، العدد السابع، دون سنة نشر.
6. عبد الله أحمد مطر الفلاسي، المسؤولية الجنائية الناتجة عن أخطاء الذكاء الاصطناعي، المجلة القانونية، مجلة متخصصة في الدراسات والبحوث القانونية، دون دار نشر، دون سنة نشر.
7. علي أحمد إبراهيم، تطبيقات الذكاء الاصطناعي في مواجهة الجرائم الإلكترونية، المجلة القانونية، دون عدد، دون سنة نشر.
8. عبد الحليم موسى يعقوب، الإعلام الجديد والجريمة الإلكترونية، الدار العالمية للنشر، السعودية، 2014م.
9. عمار ياسر زهير البابلي، دور أنظمة الذكاء الاصطناعي في التنبؤ بالجريمة، مجلة الأمن والقانون، أكاديمية دبي للنشر، الإمارات، المجلد 29، العدد 1، 2021.
10. الجرائم الإلكترونية، إعداد اللجنة العلمية بمعهد الكويت للدراسات القضائية والقانونية، 2019م.

رابعًا: المؤتمرات العلمية

1. الذكاء الصناعي، مركز البحوث العربية، لسنة 2021م.
2. عبد الله شرف الغامدي، الهيئة السعودية للبيانات والذكاء الاصطناعي، سلسلة الأدلة الإرشادية 1، السعودية، 2022م.
3. الملتقى الوطني آليات مكافحة الجريمة الإلكترونية في التشريع الجزائري، الجزائر، 2017م.
4. علي شريف، دور الذكاء الاصطناعي في نشر وتعزيز ثقافة السلام في مناطق النزاعات المسلحة، 2021م.
5. الذكاء الاصطناعي، مركز البحوث، دبي، 2021م.

خامسًا: النصوص القانونية

1. نظام مكافحة الجرائم المعلوماتية السعودي، أقره المجلس الوزاري في 1428هـ.
2. المادة (53 من الدستور اليمني.
3. المادة (255 من قانون العقوبات اليمني.

سادساً: المواقع الإلكترونية

1. نسيم رمضان، صحيفة الشرق الأوسط العرب الأولى، تاريخ الزيارة 2024/4/11م وقت الزيارة 10 مساءً على الرابط: https://aawsat.com.