دور خوارزميات الذكاء الاصطناعي فى التنبؤ بالجرائم الإرهابية الإلكترونية

هبه رمضان رجب يحى*

DOI:10.15849/ZJJLS.240330.20

* القانون المدني،، كلية الحقوق، جامعة بنى سويف، مصر.
* للمراسلة: Hebasalama12102017@gmail.com

الملخص

يعد الإرهاب الإلكتروني من أخطر أنواع الإرهاب انتشـــارا، فهو أشـــد خطورة من الإرهاب التقليدي، فقد وجد الإرهابيون ضالتهم في التكنولوجيا الرقمية، وتم استخدام مواقع الإنترنت فى الإعداد للعمليات الإرهابية، وغدت البيئة الرقمية من أبرز الوسائل المستخدمة في الإرهاب. وقد أدت الهجـــمات الإرهابية إلى تغييـــر فلســـفة الأجهـزة الشرطـية، فتم الانتقال مـن التركيـز علـى مقاضـاة السلوك الإجرامـي إلى محاولـة منع ارتكابه، من خلال تبني الشـرطة التنبؤية التى تقودها الاستخبارات، وباستخدام تقنيات الذكاء الاصـطناعي فى جمع حلول التنبؤ للوقاية من الجرائم، حيث تلعب خوارميات الذكاء الاصـــطناعي دورا بارزا فى المجال الأمني بصـــفة عامة، وفى الوقاية من الإرهاب الإلكتروني بصـــفة خاصـــة. وتهدف الدراســـة إلى بيان ماهية الخوارزميات الذكية، والتعرف على دورها فى التنبؤ بالجرائم الإرهابية، وإلى إبراز التحديات التى تواجهها، هذا وتثير الدراسة تساؤلات عديدة حول الدور البارز للخوارزميات فى التنبؤ بالإرهاب الإلكتروني؟ وحدود استخدامها؟ والتحديات التى تواجهها؟ وصولا إلى نتائج وتوصيات الدراسة.

الكلمات الدالة: التنبؤ – الإرهاب الإلكتروني– الخورازميات– التنقيب عن البيانات.

The Role of Artificial Intelligence Algorithms in Predicting Cyber Terrorist Crimes

Heba Ramadan Ragab Yehia *

Civil Law Department, Faculty of law, Beni suef University, Egypt*

*** Crossponding author:** **Hebasalama12102017@gmail.com**

Abstract

Cyber terrorism is one of the most dangerous and widespread types of terrorism, Terrorists have found what they are seeking in digital technology and the digital environment has become one of the most prominent means used in terrorism. Terrorist attacks have changed the philosophy of police agencies, moving from focusing on prosecuting criminal behavior to trying to prevent its commission, by adopting intelligence-led predictive policing and using artificial intelligence techniques, Where AI algorithms play an important role in the security field, and in the prevention of cyber terrorism. The study aims at clarifying the nature of smart algorithms, identify their role in predicting terrorist crimes and highlight the challenges they face, the study raises many questions about the prominent role of algorithms in predicting electronic terrorism? What are the limits of it use? And the challenges it faces?

Keywords: Prediction, Electronic terrorism, Algorithms, Data mining.

.

المقدمة

مع انتشار التقنيات الحديثة لنظم الاتصالات وتكنولوجيا المعلومات، وتوسع شبكة الإنترنت وشيوعها، نشأت أبعاد جديدة للإرهاب تعتمد على استخدام تلك التقنيات على الفعل المادي التقليدي، الأمر الذي أفرز صورا جديدة للإرهاب تمثلت فى الإرهاب الإلكتروني[1].

ويعد استخدام خوارزميات الذكاء الاصطناعي في التنبؤ بالجرائم الإرهابية الإلكترونية جزءا من التحول من النهج التفاعلي إلى النهج الوقائي لمكافحة الإرهاب، وقد أثيرت فكرة استخدام الحواسيب الآلية والشبكات فى القيام بالهجمات الإرهابية بعد أحداث 11 سبتمبر 2001 الذى يعد أول هجوم إرهابي إلكتروني، استخدام فيه الإرهابيون الفضاء الإلكتروني فى تنفيذ هجماتهم الإرهابية[2].

وقد انعكس النهج الوقائى لمكافحة الإرهاب بعد هذه الأحداث على تشريعات الدول، واعتمدت الدول تشريعات متعددة بشأن مكافحة الإرهاب، تجرم فيها السلوك الإرهابي فى مراحله الأولية، وذلك بتجريم مجرد التعريض للخطر وتهديد الأفراد، أو تجريم الغرض الذى من أجله يتم ارتكاب الفعل الإرهابي، على سبيل المثال اعتماد الولايات المتحدة الأمريكية: لقانون الدعم المادى الذى يُحمل الأفراد المسئولية الجنائية عن تقديم الدعم المادى لمجموعة من الأنشطة، بصرف النظر عن اتجاه نية الفرد نحو دعم الأنشطة الإرهابية، فقد أعطت هذه التشريعات للدول إمكانية الاحتجاز السابق للمحاكمة، وحق اتخاذ التدابير الإدارية بدءا من أوامر المراقبة وقيود الانتقال والحرمان من المزايا الاجتماعية وإسقاط الجنسية فى بعض الأحيان، وفى فرنسا: تم إقرار قانون فى أكتوبر 2017 بشأن استخدام التدابير الإدارية كوسيلة لأغراض مكافحة الإرهاب، لكن هذه التدابير عادة ما يتم استخدامها خارج نظام العدالة الجنائية، كما أنها قد أخذت طابعا شبه عقابى، الأمر الذى أدى إلى نقد هذه التطورات التشريعية، بسبب اتجاهها نحو المعاقبة على السلوك فى مرحلة ما قبل ارتكاب الجريمة، الأمر الذى قد ينطوى على تقويض لسيادة القانون ومساس بالحقوق الأساسية للإنسان، لكن الدول قد وضعت هذه الانتقادات جانبا، وعززت من تحركها نحو اتباع نهج وقائى لمكافحة الإرهاب من خلال استخدام تقنيات الذكاء الاصطناعي فى أنشطتها الوقائية[3].

---

[1] مخلف، مصطفى سعد حمد، جريمة الإرهاب عبر الوسائل الإلكترونية، دراسة مقارنة بين التشريعين الأردنى والعراقى، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، 2017، ص 8.

[2] نسيمة، مالك، عبدالنور، بعجى، الإرهاب الإلكترونى بين عولمة الجريمة وضرورة المكافحة، مج 7، ع 2، مجلة الدراسات والبحوث القانونية، كلية الحقوق، جامعة الجزائر، 2022، ص 65.

[3] Andrea Bianchi, Ann Greipl, States Prevention of Terrorism and the Rule of Law: Challenging the "magic" of states-/publication/www.icct.nl// Article at ICCT, 17 Nov 2022,, available at: https: Artificial Intelligence (AL), prevention-terrorism-and-rule-law-challenging-magic-artificial-intelligence-ai.

أهمية البحث

لاشك أن التنبؤ يعد أمرا أساسيا لمكافحة الإرهاب الإلكتروني، ولن يتم التنبؤ إلا من خلال استخدام خوارزميات الذكاء الاصطناعي فى تحليل أكبر قدر من البيانات ومعالجتها، وصولا إلى النتائج التى تسهم فى اتخاذ القرارات الأمنية، وبالتالى التنبؤ بالعمليات الإرهابية الإلكترونية ومنع وقوعها.

أهداف البحث

يهدف البحث إلى بيان ماهية خوارزميات الذكاء الاصطناعي، والتعرف على الدور الفعال الذى تلعبه فى مكافحة الإرهاب الإلكتروني، وبيان حدود استخدامها، وكذلك التطبيقات المستخدمه فى مواجهته، وبيان التحديات التى تواجه الذكاء الاصطناعي فى التنبؤ بجرائم الإرهاب الإلكتروني.

منهج البحث

اعتمدت الدراسة على المنهج التحليلى المقارن ببعض التشريعات لبيان الدور البارز لخوارزميات الذكاء الاصطناعي فى التنبؤ بالإرهاب الإلكتروني، وكذلك بيان حدود استخدامه، والتطبيقات المستخدمة، والتحديات التى تواجهه.

مشكلة البحث

يثير البحث العديد من التساؤلات حول:

1- ماهية خوارزميات الذكاء الاصطناعي المستخدمة فى التنبؤ بالإرهاب الإلكتروني؟

2- ما هي حدود استخدامه فى التنبؤ بالإرهاب الإلكتروني؟

3- ما هي التطبيقات الذكية المستخدمة فى التنبؤ بالإرهاب الإلكتروني؟

4- ما هي التحديات التى تواجه استخدام الخوارزميات فى التنبؤ بالجرائم الإرهابية الإلكترونية؟

خطة البحث

المبحث الأول: المقصود بخوارزميات الذكاء الاصطناعي وحدود استخدامها فى التنبؤ بالجرائم الإرهابية الإلكترونية.

المطلب الأول: ماهية خوارزميات الذكاء الاصطناعي وأهمية استخدامها فى التنبؤ بالإرهاب الإلكتروني.

المطلب الثانى: حدود استخدام خوارزميات الذكاء الاصطناعي فى التنبؤ بالإرهاب الإلكتروني.

المبحث الثانى: خوارزميات الذكاء الاصطناعي ودورها فى التنبؤ بالجرائم الإرهابية الإلكترونية.

المطلب الأول: تطبيقات الذكاء الاصطناعي فى التنبؤ بالجرائم الإرهابية الإلكترونية.

المطلب الثانى: التحديات التى تواجه الخوارزميات الذكية فى مكافحة الجرائم الإرهابية الإلكترونية.

المبحث الأول: المقصود بخوارزميات الذكاء الاصطناعي وحدود استخدامها فى التنبؤ بالجرائم الإرهابية الإلكترونية

تلعب تقنيات الذكاء الاصطناعي وخوارزمياته دورا هاما فى الحصول على الاستنتاجات الأمنية التى تفيد فى التنبؤ بالجرائم ومنع وقوعها، من خلال العمل على تحليل قواعد البيانات الأمنية[1]، كما يمكنه التنبؤ بالإرهاب الإلكتروني بناء على البيانات الوصفية لنظم الاتصالات والمعلومات، والمعاملات المالية، وأنماط السفر، ونشاط تصفح الإنترنت، بالإضافة إلى المعلومات المتاحة للجمهور[2]، فالتنبؤ الجيد ضروري لوضع استراتيجية لمكافحة الإرهاب الإلكتروني، بحيث يساعد على منع الإرهاب، دون التعدى غير المبرر على حقوق الأفراد، لذا سوف نتناول فى المطلبين الآتيين: ماهية خوارزميات الذكاء الاصطناعي وحدود استخدامه فى التنبؤ بالإرهاب الإلكتروني، وذلك على الوجه الآتى:

المطلب الأول: ماهية خوارزميات الذكاء الاصطناعي وأهمية استخدامها فى التنبؤ بالإرهاب الإلكتروني

أولا: ماهية خوارزميات الذكاء الاصطناعي

تعرف الخوارزمية بأنها: "عملية منظمة أو مجموعة من القواعد التى يجب اتباعها لحل المشكلات، فهى تتابع فى خطوات منطقية"، وهذا هو جوهر العمليات المبرمجة فى أجهزة الحاسب الآلى، فأجهزة الحاسب الآلى تعتبر أجهزة تحويلية فى العديد من المجالات، فهى قادرة ميكانيكياً على أداء الوظائف بسرعة كبيرة من خلال معالجة كميات ضخمة من البيانات[3].

أما عن الذكاء الاصطناعي فهو أحد فروع علوم الحاسب الآلى، وأحد الركائز الرئيسية التى ترتكز عليها صناعة التكنولوجيا فى عصر التكنولوجيا الرقمية، حيث يهدف إلى فهم طبيعة الذكاء الإنسانى عن طريق عمل برامج للحاسب الآلى تكون قادرة على محاكاة السلوك الإنسانى الذى يتسم بالذكاء[4].

كما أنه أحد أهم مخرجات الثورة الصناعية الرابعة، لتعدد استخداماته فى مختلف المجالات الأمنية والعسكرية والصحية والاقتصادية والتعليمية والخدمية، إلخ..[5].

---

[1] شادى عبد السلام، حروب الجيل الخامس، أساليب التفجير من الداخل على الساحة الدولية، مركز المستقبل للأبحاث والدراسات المتقدمة، الإمارات، 2020، ص5.

[2] Kathleen Mckendrick, Artificial Intelligence Prediction and counterterrorism, International Security Department, August 2019, p.12.

[3] مصبح، عمر عبدالمجيد عبدالحميد، توظيف خوارزميات العدالة التنبؤية فى نظام العدالة الجنائية "الآفاق والتحديات"، مج 10، ع 1، المجلة الدولية للقانون، جامعة قطر، 2021، ص 237.

[4] مصبح، عمر عبدالمجيد عبدالحميد، مرجع سابق، ص 238.

[5] أبو النجا، محمد عبدالحكيم محمد، دور الاستراتيجيات الأمنية لمواجهة جرائم الذكاء الاصطناعي وتكنولوجيا المعلومات، عدد خاص بالمؤتمر الدولى السنوى العشرون، مجلة البحوث القانونية والاقتصادية، 2021، ص 927.

فمنذ منتصف القرن العشرين شهد الحاسب الآلى تطورات كبيرة، أصبح بموجبها قادرا على القيام بمهام أكثر تعقيدا مما نعتقد، حيث يمكنه إثبات النظريات الرياضية المعقدة، والقيام بالعمليات الإحصائية، ولديه سرعة معالجة عالية، وسعة تخزينية كبيرة[1].

ويعرف الذكاء الاصطناعي بأنه: "ذلك العلم الذى يقوم على استنباط نظم قادرة على درسة المشاكل وحلها، والقيام بأداء الوظائف بمحاكاة العمليات الذهنية دون أى تدخل بشرى، بحيث يمكنها بلوغ مستويات التشغيل الذاتى، وأن تتصرف باستقلالية تامة[2].

كما يُعرف بأنه: قدرة أجهزة الحاسب الآلى والآلات الرقمية على أداء مهام معينة، تحاكي وتماثل تلك التى يقوم بها الإنسان، كقدرته على التفكير والتعلم والإستنتاج ورد الفعل واتخاذ القرارات بوعى وذكاء[3].

ويبرز دور الذكاء الاصطناعي فى المجال الأمني، كأحد الركائز الأساسية التى تعتمد عليها الأجهزة الأمنية فى التنبؤ بالجرائم، حيث يقوم الذكاء الاصطناعي باستخدام الخوارزميات الرياضية فى القيام بعمليات حسابية واستنتاجية لمساعدة الأجهزة الأمنية فى وضع الخطوط العرضية لمواجهة الإرهاب الإلكتروني، عن طريق اكتشاف الاستباقات المعلوماتية واستنتاجها، وتحديد أماكن الجريمة والتنبؤ بوقوعها[4].

ثانيا: أهمية استخدام الذكاء الاصطناعي فى التنبؤ بالإرهاب الإلكتروني:

كان الإرهاب وما زال يشكل خطرا حقيقيا يهدد كافة الدول، بصفة خاصة دول الشرق الأوسط، وذلك بسبب التطورات التى تشهدها تلك الدول على الصعيد السياسى والاقتصادي، فلم تعد تنحصر أنشطة الإرهاب داخل حدود الدولة الواحدة، وامتدت لتشمل مساحات شاسعة، وساعد على ذلك استخدام التقنيات التكنولوجيا الحديثة خصوصا الإنترنت ومواقع التواصل الاجتماعي، فى تحويل الأفكار المتطرفة إلى واقع ملموس، تمثل ذلك فى الجرائم الإرهابية الإلكترونية، فقد أسهمت تلك التقنيات في ارتكاب جرائم إرهابية عابرة للحدود الزمنية والمكانية[5].

والتنبؤ بمكافحة الجرائم الإرهابية الإلكترونية يتطلب نوعا من الذكاء الاصطناعي يتيح استخراج المعرفة واكتشافها والتنبؤ بها من خلال البيانات الرقمية الضخمة، واستخدام خوارزميات الذكاء الاصطناعي التى تدعم النماذج التنبؤية المبرمجة ذاتيا على التعامل مع البيانات، وفى كثير من الأحوال لا يمكن تحليل البيانات بدون هذا النهج، كما لا يمكن بناء النماذج بدون هذه البيانات[6].

---

[1] البابلى، عمار ياسر محمد زهير، دور أنظمة الذكاء الاصطناعي فى التنبؤ بالجريمة، مج 29، ع 1، مجلة الأمن والقانون، أكاديمية شرطة دبى، 2021، ص 140.

[2] الشرايرى، محمد أحمد، المسئولية المدنية الذكية عن أضرار الذكاء الاصطناعي، دراسة مسحية مقارنة، ع2، ع تسلسلى 38، مجلة كلية القانون الكويتية العالمية، مارس 2022، ص 364.

[3] مرعى، أحمد لطفى السيد، انعكاسات تقنيات الذكاء الاصطناعي على نظرية المسئولية الجنائية، دراسة تأصيلية مقارنة، ع 80، مجلة البحوث القانونية والاقتصادية، يونيو 2022، ص 256.

[4] البابلى، عمار ياسر محمد زهير، دور أنظمة الذكاء الاصطناعي فى التنبؤ بالجريمة، مرجع سابق، ص 128.

[5] العامرى، سامر سعدون عبود، التحريض على ارتكاب الجرائم الإرهابية باستخدام وسائل التقنية الحديثة، ع 1، كلية القانون، جامعة بغداد، 2016، ص 567.

[6] راشد، باسم، التنبؤ بالهجمات: فرص ومخاطر استخدامات الذكاء الاصطناعي فى مكافحة الإرهاب، مركز المستقبل للأبحاث والدراسات المتقدمة، بتاريخ 9 أكتوبر 2019، على الرابط الآتى:
%D8%./50022/Item/Mainpage/ar-AE/futureuae.com//https:

وقد ظهرت عبارة الإرهاب الإلكتروني لأول مرة فى منتصف الثمانينات فى دراسة للباحث "Barry Collin" الذى توصل فيها إلى صعوبة تعريف الإرهاب الإلكتروني، وصعوبة تحديد دور كل من الحاسب الآلى والإنترنت فى القيام بالعمل الإرهابي، وفى عام 1980 تم استخدام هذا المصطلح للإشارة إلى الهجمات الإلكترونية على اقتصاد الولايات المتحدة الأمريكية، واتضح ذلك فى تقرير الأكاديمية الوطنية الأمريكية للعلوم، الذى ذُكر فيه: "أن الولايات المتحدة الأمريكية فى خطر لاعتمادها بشكل متزايد على أجهزة الحاسب الآلى فى إدارة الخدمات الحيوية، الذى يجعلها عرضة لهجوم إلكتروني متعمد؛ وهذا ما يجعل من إرهابي الغد قادرا على إحداث المزيد من الضرر باستخدام لوحة المفاتيح أكثر من القنابل"[1].

وقد اختلفت الآراء الفقهية والتشريعات الوطنية بشأن تعريف الإرهاب، لأن مصطلح الإرهاب قد يكون له عدة مدلولات سياسية وقومية ودينية تختلف من دولة لأخرى، فلا يوجد تعريف جامع مانع له، إلا أنه قد تم الاتفاق على عدد من العناصر التى يلزم أن يشتمل عليها التعريف وهى: استخدام القوة أو التهديد باستخدامها، بما يؤدى إلى قتل أو تخويف وترويع المدنيين.

فقد عرفت الاتفاقية العربية لمكافحة الإرهاب الصادرة فى 22 أبريل 1998، عن مجلس وزراء الداخلية والعدل العرب فى المادة الأولى منها الإرهاب بأنه: "كل فعل من أفعال العنف والتهديد، أيا كانت بواعثه أو أغراضه، يقع تنفيذا لمشروع إجرامى فردى أو جماعى، ويهدف إلى إلقاء الرعب بين الناس، أو ترويعهم بإيذائهم، أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر، أو إلحاق الضرر بالبيئة، أو بأحد المرافق أو الأملاك العامة، أو احتلالها أو الاستيلاء عليها، أو تعريض أحد الموارد الوطنية للخطر"[2].

فقد استخدم الإرهابيون التقنيات الحديثة مثل الهواتف المحمولة، والحواسب الآلية، وشبكات الإنترنت وما ينطوى عليه من مواقع إلكترونية ووسائل للتواصل الاجتماعي وتطبيقات عديدة كالبريد الإلكتروني، تمكنهم من التواصل والاتصال ببعضهم بعضا من أى مكان فى العالم، بأسرع الطرق وأوفرها، وتحقيق أهدافهم الإجرامية، وإخفاء معالم جرائمهم، حيث يصعب تتبع مرتكبيها.

أما عن الإرهاب الإلكتروني أو المعلوماتى فهو أحد صور الجرائم الإرهابية انتشارا فى الوقت الحالى، وهو نوع من الإرهاب الحديث الذى يستثمر تقنيات المعلومات والاتصالات ويوظفها بشكل يلائم متطلباته[3]، حيث يقوم على استخدام برمجيات الحاسب الآلى وإمكاناته فى ترويع الآخرين، دون اللجوء إلى العنف الجسدى أو المادى، كاختراق المواقع الإلكترونية والدخول على الشبكات والعبث فى محتوياتها بهدف تدميرها أو تعطيلها، واستخدام البريد الإلكتروني فى إرسال رسائل تهديدية أو فى نشر الأكاذيب، بهدف نشر الفوضى وإرباك الاستقرار الأمني فى البلاد، فالإرهاب الإلكتروني يختلف عن الإرهاب التقليدي فى استخدامه للتقنيات الحديثة فى ارتكاب الجرائم الإرهابية، مع حفاظه على الصفات العامة للإرهاب[4].

---

[1] نسيمة، مالك، عبدالنور، بعجى، الإرهاب الإلكترونى بين عولمة الجريمة وضرورة المكافحة، مرجع سابق، ص 67.

[2] العامرى، سامر سعدون عبود، مرجع سابق، ص 575.

[3] مخلف، مصطفى سعد حمد، مرجع سابق، ص 3.

[4] العامرى، سامر سعدون عبود، مرجع سابق، ص 581-582.

ويعرف الإرهاب الإلكتروني بأنه: "العدوان أو التخويف أو التهديد المادى أو المعنوى، باستخدام الوسائل الإلكترونية من قبل الدول أو الجماعات أو الأفراد على الإنسان فى نفسه أو ماله أو دينه أو عقله أو عرضه، بغير حق وبشتى أصناف العدوان وصور الإفساد فى الأرض"[1].

كما يعرف الإرهاب الإلكتروني بأنه: العدوان أو التخويف أو التهديد المعنوى أو المادى الصادر من الإرهابيين، باستخدام الوسائل الإلكترونية، بهدف الإخلال بالنظام العام والأمن وإلحاق الضرر بالممتلكات، والاستيلاء على الأموال العامة والخاصة للدولة[2].

وقد عرفته الفقرة (هـ) من المادة الثالثة من قانون منع الإرهاب الأردني 18 لسنة 2014 بأنه: استخدام نظام المعلومات أو الشبكة المعلوماتية، أو أي وسيلة نشر أو إعلام أو إنشاء موقع إلكتروني، لتسهيل القيام بإعمال إرهابية أو دعم لجماعة أو تنظيم أو جمعية تقوم بإعمال إرهابية، أو الترويج لأفكارها أو تمويلها، أو القيام بأي عمل من شأنه تعريض الأردنيين أو ممتلكاتهم لخطر أعمال عدائية أو انتقامية تقع عليهم.

وعددت المادة (15) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[3]الإرهاب الإلكتروني، وحصرته فى استخدام تقنية المعلومات فى الأعمال الإرهابية، بذكر الآتى: "الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات:

1- نشر أفكار ومبادئ جماعات إرهابية والدعوة إليها.
2- تمويل العمليات الإرهابية والتدريب عليها، وتسهيل الاتصالات بين التنظيمات الإرهابية.
3- نشر طرق صناعة المتفجرات التى تستخدم خاصة فى عمليات إرهابية.
4- نشر النعرات والفتن والاعتداء على الأديان والمعتقدات.

وعليه يمكننا القول بأن الإرهاب الإلكتروني هو: نوع من أنواع الإرهاب الذى يعتمد على الأساليب التكنولوجية الحديثة فى تنفيذ هجماته، ويعتمد بشكل أساسى على شبكات المعلومات، ويهدف إلى ترويع الأفراد وتهديد أمنهم واستقرارهم وإلحاق الضرر بهم.

فهذه العمليات الإرهابية الإلكترونية يمكن أن تتم في أي لحظة، وأن تنطلق من أي مكان في العالم، كأن تتم من البيت أو المكتب، ودون الحاجة إلى أى تكاليف، على خلاف العمليات الإرهابية التقليدية التى تتم من خلال الهجمات أو الاختراقات الفعلية والتعامل مع المتفجرات، كما يمكن أن يقوم بها ممثلون حكوميون أو غير حكوميين، أفراد أو جماعات، كما أن عدد الأهداف التي يتم تحقيقها كبيرة، وتحقق خسائر هائلة، وبتكلفة زهيدة[4].

ومن أمثلة الجرائم الإرهابية الإلكترونية قيام الإرهابيين بوضع قنابل إلكترونية موقوتة فى عدد من الأماكن وربطها ببعضها، بحيث ترسل شفرات إلكترونية عن بعد لتفجيرها فى آن واحد، أو قيامهم باختراق الشبكات أو المواقع

---

[1] ناجى، إسلام محروس، جرائم الإرهاب الإلكترونى، دراسة تأصيلية تحليلية للتشريع السعودى، ع 93، مجلة القانون والاقتصاد، كلية الحقوق، جامعة القاهرة، 2017، ص 500.

[2] مخلف، مصطفى سعد حمد، مرجع سابق، ص 18.

[3] وافق عليها مجلسى وزراء الداخلية والعدل العرب فى اجتماعهما المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة، بتاريخ 12/21/ 2010م.

[4] البداينة، ذياب موسى، دور الأجهزة الأمنية فى مكافحة جرائم الإرهاب المعلوماتى، ورقة عمل مقدمة فى الدورة التدريبية بعنوان مكافحة الجرائم الإرهابية المعلوماتية فى الفترة من 9-4/13/ 2006، كلية التدريب، جامعة نايف العربية للعلوم الأمنية، المغرب، 2006، ص 7.

الإلكترونية الحكومية، أو اختراق مصانع الأدوية وتغيير تركيبات الأدوية بها، أو اختراق أجهزة استشعار الطائرات والتسبب فى وقوعها، أو فى مهاجمة نظم المراقبة الجوية[1].

ومن أهم مبررات استخدام خوارزميات الذكاء الاصطناعي فى التنبؤ بالجرائم الإرهابية الآتى:

- تعد الخوارزميات تقنية هامة تفيد فى التنبؤ بالجرائم، من خلال استخدام كميات هائلة من البيانات لتدريب خوارزميات مكافحة الإرهاب الإلكتروني باستمرار، للتنبؤ بالأنماط غير المعروفة والتعرف عليها، فهذه الخوارزميات تستخدم على نطاق واسع في جميع مراحل نظام العدالة الجنائية، ومن أكثر الخوارميات شيوعا: خوارزميات "تقييم المخاطر قبل المحاكمة" التى يتم استخدامها في أغلب الولايات الأمريكية.
- تسهم تقنية الخوارزميات في الحفاظ على الخبرات الإنسانية، من خلال نقلها إلى الآلات الذكية؛ وتغذيتها باللغة البشرية لاستخدامها في التعامل مع الآلات، كما أنها تستخدم في المراحل الإجرائية التي يتم فيها صنع القرار، كونها تمتاز بالموضوعية والاستقلالية، وتجنب الأفراد الضغوط النفسية والعصبية، فهى تساعدهم على توفير الوقت والجهد، لذلك يتم استخدامها فى القيام بالأعمال الخطرة والمشاركة في عمليات الإنقاذ أثناء الكوارث وفى التنبؤ بالجرائم، أضف إلى ذلك الدور الفعال الذى سوف تلعبه فى "القطاعات التي تحتوي على مهام عديدة تتميز بالتعقيد، وتحتاج إلى تركيز ذهني وعقلي متواصل، واتخاذ قرارات سريعة وحساسة، لا تحتمل التأخير أو الخطأ"، كما فى المجال الأمني خصوصا فى مكافحة الجرائم الإرهابية[2].

المطلب الثانى: حدود استخدام خوارزميات الذكاء الاصطناعي فى التنبؤ بالإرهاب الإلكتروني.

لاشك أن التكنولوجيا سلاح ذو حدين فكما يمكن استخدامها فى ارتكاب الجرائم، فإنها كذلك تستخدم فى منع الجريمة والكشف عنها، وهذه الازدواجية كانت موضــع اهتمام الفريق المعني بالتعاون الرقمي الذي أنشــأه الأمين العام للأمم المتحدة عام ٢٠١٨، بشأن تعزيز التعاون الدولي والتعاون بين أصــحاب المصلحة المتعددين، والمساهمة في المناقشة العامة بشأن مستقبل رقمي آمن وشامل للجميع، حيث قام بتسليط الضوء عليها في تقريره "عصر الترابط الرقمي"، حيث ذكر أن: "التكنولوجيات الرقمية أثبتت أنها قادرة على ربط الأفراد، عبر الحواجز الثقافية والجغرافية مما يزيد التفاهم، ويحتمل أن يساعد المجتمعات على أن تصبح أكثر سلاماً وتماسكاً، ورغم ذلك فإن هناك تكنولوجيات رقمية تُستخدم لانتهاك الحقوق الأساسية للإنسان، وتقويض الخصوصية، واستقطاب المجتمعات، والتحريض على العنف".

وعلى ذلك فالذكاء الاصطناعي أيضا يعد سلاحا ذا حدين، فكما يمكن استخدامه فى القيام بالهجمات الإرهابية الإلكترونية، وهو مايعزز من ظهور أشكال جديدة للجريمة، فإنه يمكن استخدامه أيضا فى التنبؤ بالجرائم الإرهابية الإلكترونية[3].

---

[1] إبراهيم، على أحمد، تطبيقات الذكاء الاصطناعي فى مواجهة الجرائم الإلكترونية، مج 9، ع 8، المجلة القانونية، 2021، ص 2822.

[2] مصبح، عمر عبدالمجيد عبدالحميد، مرجع سابق، ص 238.

[3] ورقة معلومات أساسية أعدتها الأمانة العامة للأمم المتحدة بعنوان: التعاون الدولى وتقديم المساعدة التقنية من أجل منع الجرائم بجميع أشكالها والتصدى لها، مؤتمر الأمم المتحدة الرابع عشر لمنع الجريمة والعدالة الجنائية، كيوتو، اليابان، 20–27 أبريل 2020، ص 2، 16.

فالجرائم الإرهابية الإلكترونية قد تعتمد فى هجومها على استخدام الذكاء الاصطناعي والحوسبة السحابية وإنترنت الأشياء، فتستخدم البرمجيات الخبيثة لاختراق أنظمة أمن الشبكات والحاسبات، وأجهزة التنصت، لتسخيرها فى القيام بالعمليات الإرهابية الإلكترونية، كما تستخدم الفضاء الإلكتروني فى القيام بالعمليات المشبوهة دون علم أصحابها فيما يعرف "بالشبكات الآلية"، وشن هجمات متنوعة مثل الهجمات الموزعة على المواقع المستهدفة لأغراض إجرامية كالإرهاب والتهديد والتخريب، فلم تعد هجمات الإرهابيين تعتمد على الأفعال الإرهابية المادية واستخدام القوة العسكرية، وأصبحت الهجمات أكثر براعة واكتسبت اتجاها تقنيا، فلم تعتد تقتصر هجماتهم على التدريب والتمويل والتخطيط، وتطورت لتهديد الأفراد ومهاجماتهم من خلال شبكات الإنترنت، مع إمكانية إخفاء معالم جريمتهم باستخدام التقنيات الحديثة، على سبيل المثال: فقد تعرضت المملكة العربية السعودية عام 2016 لهجوم إلكتروني استهدف البنية التحتية بها، لمحاولة سرقة البيانات الخاصة بها، كما تعرضت مصر عام 2018 وفق التقرير الصادر من شركة تريند مايكرو عام 2021 للعديد من الهجمات الإلكترونية، فقد زادت عدد البرمجيات الخبيثة بشكل كبير بنسبة 25% فى الربع الأخير من عام 2017، بحيث تأتى مصر فى المرتبة الثالثة على مستوى القارة الأفريقية، من حيث تعرضها للبرمجيات الخبيثة والتهديدات الإلكترونية[1]، حيث تعرضت المؤسسات الحكومية المصرية عام 2020 لنحو 42 مليون هجمة إلكترونية، وقد استطاعت المؤسسة الأمنية التصدى لتلك التهديدات من خلال استخدام الخوارزميات الذكية فى منع التهديدات المحتملة[2].

ورغم فوائد إدخال تقنيات الذكاء الاصطناعي واستخدامها فى التنبؤ بالجرائم الإرهابية الإلكترونية إلا أن ذلك سيكون مصحوبا بخطر كبير، يتمثل ذلك الخطر فى تقويض سيادة القانون وحقوق الإنسان، فالتنبؤ بالذكاء الاصطناعي يبرر اتخاذ تدابير إدارية، تلك التدابير التى وإن كانت تعد أداة مشروعة ومفيدة للحد من المخاطر التى تهدد الأمن القومى، وتساعد على خلق بيئة أكثر أمانا، إلا أن استخدامها فى البحث عن الأمن لا ينبغى أن يقوض من سيادة القانون وحقوق الإنسان[3]، تلك الحقوق التى نص عليها فى الإعلان العالمى لحقوق الإنسان، وتم توحيدها فى المعاهدات، مثل معاهدة العهد الدولى الخاصة بالحقوق المدنية والسياسية عام 1966 التى دخلت حيز النفاذ عام 1976.

فخوارزميات الذكاء الاصطناعي التى تستخدم من قبل أجهزة إنفاذ القانون فى التنبؤ بالجرائم الإرهابية الإلكترونية، قد يكون من شأنها أن تؤثر على الحقوق والحريات المدنية للأفراد، كما يمكنها أن تقوض من حق المتهم في افتراض البراءة، كما قد يؤدي استخدام الخوارزميات غير الشفافة إلى تفاقم العلاقة بين أفراد المجتمع ورجال إنفاذ القانون، وكذلك إلى التمييز العنصرى ضد جماعات أو طوائف معينة[4].

---

[1] محمود، رانيا سليمان أبو المعاطى، والدسوقى، نهى محمد إبراهيم، والصفتى، فاتن فايز حميدة، سياسة مكافحة الإرهاب الإلكترونى، مصر والسعودية أنموذجا، ع 53، المركز العربى للبحوث والدراسات، آفاق سياسية، 2020، ص 52، 53.

[2] الداغر، مجدى، اتجاهات النخبة نحو توظيف الإعلام الأمنى لتطبيقات الذكاء الاصطناعي فى مكافحة الجرائم الإلكترونية وانعكاساته على دعم وتعزيز الأمن السيبرانى فى مصر، ع 33، المجلة العربية لبحوث الإعلام والاتصال، أبريل/يونيو 2021، ص 8.

[3] Tanya Mehra, Matthew Wentworth, and Bibi Van Ginkel, The Expanding Use of Administrative Measures in a Counter-Terrorism Context- Part 1: In Need of Rule of Law Safeguards, Article in ICCT, 10 Nov 2021, available at: https://www.icct.nl/publication/states-prevention-terrorism-and-rule-law-challenging-magic-artificial-intelligence-ai.

[4] ACLU, "Statement of Concern About Predictive Policing by ACLU and 16 Civil Rights Privacy, Racial Justice, and Technology Organizations", August 31 2016, available at: https://www.aclu.org/other/statement-concern-about-predictive-policing-aclu-and-16-civil-rights-privacy-racial-justice .

ولما كانت البيانات الشخصية المستند إليها فى المعالجة وقودا لتلك البرمجيات، فإن اللجوء إلى جمع تلك البيانات ومعالجتها للتنبؤ بوقوع جريمة إرهابية إلكترونية مستقبلية من عدمه، ينطوى على مساس بالحماية المقررة فى قوانين حماية البيانات الشخصية، على سبيل المثال: قانون حماية البيانات الشخصية المصرى 151 لسنة 2020، فالبيانات الشخصية للجماعات الإرهابية ولأفرادها هى محل تطبيقات الذكاء الاصطناعي التنبؤى[1].

وقد عرف المشرع المصرى البيانات الشخصية فى قانونه بأنها: "أى بيانات متعلقة بشخص طبيعى محدد أو يمكن تحديده، بشكل مباشر أو غير مباشر، عن طريق الربط بين هذه البيانات وأى بيانات أخرى كالاسم أو الصوت أو الصورة أو رقم تعريفى أو محدد للهوية عبر الإنترنت، أو أى بيانات تحدد الهوية النفسية أو الصحية أو الاقتصادية أو الثقافية أو الاجتماعية"[2]، فهذه البيانات الشخصية التى يحميها قانون حماية البيانات الشخصية هي جزء لا يتجزأ من البيانات التي يتم بها تغذية الذكاء الاصطناعي التنبؤى.

وقد استثنى قانون حماية البيانات الشخصية 151 لسنة 2020، البيانات الشخصية المتعلقة بمحاضر الضبط القضائى والتحقيقات والدعاوى القضائية؛ والبيانات الشخصية لدى جهات الأمن القومى وما تقدره لاعتبارات أخرى من نطاق الحماية القانونية المقررة بموجب ذلك القانون[3].

والعلة من استثناء جهات الأمن القومى من نطاق القانون 151 لسنة 2020 تتجلى في حماية الأمن القومي الذي يضطلع بمهمة التنبؤ بالجرائم ومنع وقوعها، وعليه فإن ذلك الاستثناء يعزز موقف الأجهزة الأمنية من استخدام تقنيات الذكاء الاصطناعي فى جمع ومعالجة البيانات الشخصية الخاصة بالأفراد، وبهذا الاستثناء يتضح لنا موقف القانون المصرى من استخدام الذكاء الاصطناعي فى الوقاية من الجرائم الإرهابية الإلكترونية، فقد أصبحت هناك أرض خصبة لاستخدام تقنيات الذكاء الاصطناعي في التنبؤ بالجرائم.

كذلك الأمر فى الإمارات العربية المتحدة فقد حظر المشرع الإماراتى جمع أو حفظ أو تخزين أو معالجة البيانات الشخصية الخاصة بالأفراد، والمنصوص عليها فى القانون الاتحادى رقم 45 لسنة 2021[4]، وقد عرف المشرع الإماراتى البيانات الشخصية بتعريف مشابه للتعريف الوارد فى القانون المصرى، لكنه عرف نوعين من المعالجة للبيانات الشخصية: المعالجة العادية والمعالجة المؤتمتة[5].

فتنامى استخدام تقنيات الذكاء الاصطناعي بدون ضوابط قانونية، قد ينطوى على مساس لحق الإنسان فى خصوصية[6]، ويعد ذلك انتهاكا لحرمة الحياة الخاصة به، ذلك الحق الذى كفله له القانون والدستور، فقد نص فى المادة (92) من الدستور المصرى 2014 على: عدم جواز المساس بالحقوق والحريات اللصيقة بالفرد، ومنها حق الفرد فى حرمة الحياة الخاصة، كما نص فى الفصل الثالث من قانون جرائم تقنية المعلومات 175 لسنة

---

[1] الشريف، محمود سلامة عبدالمنعم، الطبيعة القانونية للتنبؤ بالجريمة بواسطة الذكاء الاصطناعي ومشروعيته، مج 3، المجلة العربية لعلوم الأدلة الجنائية والطب الشرعى، 2021، ص 351.

[2] المادة الأولى من الفصل الأول من قانون حماية البيانات الشخصية رقم 151 لسنة 2020.

[3] المادة الثالثة من قانون حماية البيانات الشخصية 151 لسنة 2020.

[4] منشور فى الجريدة الرسمية العدد 712 (ملحق 1)، بتاريخ 2021/09/26.

[5] عرفت المادة الأولى من القانون رقم 45 لسنة 2021 المعالجة المؤتمتة بأنها:"المعالجة التى تتم باستخدام برنامج أو نظام إلكترونى يعمل بطريقة آلية وتلقائية إما بشكل مستقل كليا دون أى تدخل بشرى أو بشكل جزئى بإشراف وتدخل بشرى محدود".

[6] صدر قرار الجمعية العامة للأمم المتحدة رقم 167/68 فى ديسمبر 2014 بشأن الحق فى الخصوصية فى العصر الرقمى.

2018[1]على العقوبات المتعلقة بجرائم الاعتداء على حرمة الحياة الخاصة والمحتوى المعلوماتى غير المشروع، وعليه فإن كافة الخدمات التكنولوجية تفرض على المستخدم ضرورة الموافقة على السماح بجمع وتحليل بياناتهم الشخصية باستخدام خوارزميات الذكاء الاصطناعي[2].

فلايجوز وفقا للقانون الفرنسى اتخاذ أى قررات آلية استنادا إلى استخدام الذكاء الاصطناعي فى بعض الأغراض، وهو ما نصت عليه المادة (71) من اللائحة الأوروبية 2016/967[3]، التى استمد منها قانون المعلومات والحرية الفرنسى نصوصه، بشأن منع اتخاذ آية قرارات يمكن أن تحدث آثارا قانونية فى مواجهة شخص ما، إذا كان تدخلها الوحيد هو المعالجة الآلية للبيانات الشخصية الخاصة به، أو بتقييم بعض جوانبها، كأن يتم تحليل الجوانب المتعلقة بسلوك الفرد أو وضعه الاقتصادي أو حالته الصحية أو اهتماماته الشخصية، فلا يجوز اتخاذ أى قرارات ضده، على نحو ينتج من خلاله آثار قانونية تتعلق بالشخص المعنى بالبيانات أو تؤثر عليه تأثيرا جسيما[4].

ومع تزايد انتشـار اسـتخدام تقنيات الذكاء الاصـطناعي لدى أجهزة إنفاذ القانون، ازدادت أهمية وجود ضمانات أخلاقية، وقد اتُّخذت مبادرات ذات طابع طوعي، للتقليل من مخاطر انتهاك الحقوق الأســاســية للإنسان، والتخفيف من غموض المسئولية القانونية للاستخدام الأخلاقي للذكاء الاصطناعي، وضمان عدم إساءة استخدامها من قبل السلطة فى جمع الأدلة، من خلال الإشراف القضائي أو المستقل على استخدام هذه التقنيات، ومراعاة مبادئ الشـرعية والضــرورة والتناسـب، كما ينبغى أن تمتثل الأدلة الإلكترونية للإجراءات المتعارف عليها حتى تكون مقبولة.

وقد اقترحت فرنسا عدة ضمانات وفقا لنص المادة 2/22 من اللائحة الأوروبية 679/ 2016، منها: الحق في معرفة آليات عمل الخوارزميات، حيث يحق للشخص المعنى بالبيانات الاطلاع على آلية عمل الخوارزميات، التى تضطلع بمعالجة بياناته الشخصية.

وكذلك قامت المفوضية الأوروبية لكفاءة العدالة CEPEJ "التابعة لمجلس أوروبا" بالإعلان عن الميثاق الأخلاقي الأوروبي بشأن استخدام الذكاء الاصطناعي في النظم القضائية، وجاء في الميثاق النص على عدة مبادئ للميثاق الأخلاقى وهي: مبدأ احترام الحقوق الأساسية للإنسان، مبدأ عدم التمييز، مبدأ الجودة والأمان عن طريق استخدام بيانات من مصادر معتمدة، مبدأ الشفافية والحياد والنزاهة[5].

وفى سبيل مكافحة الإرهاب الإلكتروني قامت العديد من الدول بإصدار تشريعات خاصة لتجريمه والعمل على مكافحته، فعلى سبيل المثال: قامت المملكة العربية السعودية بإنشاء نظام مكافحة الجرائم المعلوماتية الصادر بمرسوم ملكى رقم 17م بتاريخ 25 مارس لعام 2017، وفى مصر فقد تم إصدار قانون رقم 94 لسنة 2015 بشأن مكافحة الإرهاب المعدل بالقانون رقم 15 لسنة 2020، كما نص الدستور المصرى لعام 2014 فى المادة

---

[1] الجريدة الرسمية، العدد 32 مكرر (ج) فى 14 أغسطس 2018.

[2] دهشان، يحيى، المسئولية الجنائية عن جرائم الذكاء الاصطناعي، مج 34، ع 82، مجلة الشريعة والقانون، الإمارات، أبريل 2020، ص 144.

[3] اللائحة التنظيمية الأوروبية رقم 967/ 2016، الصادرة عن البرلمان والمجلس الأوروبى فى27 أبريل 2016، التى ألغت التوجيه 46/95، ودخلت حيز التنفيذ في 25 ماى 2018، وتم إدراجها ليتم تطبيقها آليا فى التشريع الوطني لكافة دول الاتحاد الأوروبي، ووفقا للمادة (22–1، 4) يجب على مراقبى البيانات تزويد صاحب البيانات حول وجود أتمته للقرارات.

[4] Judith Rochfeld, L’encadrement des décisions prises par les algorithmes, Dalloz IP/IT, n°9, 2018, p. 475 .

[5] http://julkaisut.valtioneuvosto.f/bitstream/hadle/10024/160391/TEMrap_47_2017_verkkojulkaisu.pdf?sequence=1&isAllowed=y.

(31) منه على أن: "الفضاء المعلوماتى جزء أساسى من منظومة الاقتصاد والأمن القومى، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، على النحو الذى ينظمه القانون"، كما أصدرت مصر قانون مكافحة جرائم تقنية المعلومات 175 لسنة 2018، الذى بموجبه تم تجريم الممارسات الإلكترونية غير المشروعة، وقد انضم كلاهما للاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010[1] بهدف تعزيز التعاون بين الدول العربية لمكافحة جرائم الإرهاب الإلكتروني.

المبحث الثانى: خوارزميات الذكاء الاصطناعي ودورها فى التنبؤ بالجرائم الإرهابية الإلكترونية

يجب أن تتضمن الأجهزة الشرطية تقنيات الذكاء الاصطناعي وخوارزمياته كأحد الدعائم الرئيسية لمواجهة الجرائم الإرهابية الإلكترونية، فالذكاء الاصطناعي يساعد الأجهزة الأمنية على تطوير إمكاناتها وقدراتها من خلال استخدام[2]:

- الشرطة الرقمية: أى اعتماد الأجهزة الشرطية على التقنيات الحديثة فى جمع الأدلة الرقمية التى يمكن الحصول عليها من خلال سجلات الهاتف أو رسائل البريد الإلكتروني، واستخدام الذكاء الاصطناعي فى تحليل البيانات للمساعدة فى سرعة الوصول إلى الجناة ومنع ارتكاب الجريمة وسرعة اتخاذ القرار المناسب.
- التحقيق الرقمى: وذلك برفع الملفات الرقمية الخاصة بالأجهزة الشرطية على شبكة الإنترنت بما تحتوي عليه من أدلة جنائية، وأولى خطوات الرقمنة تكمن فى تفعيل الهوية الرقمية، وذلك من خلال إبراز هوية مستخدمى الإنترنت، فالهوية الرقمية التى يتم إثباتها تزيد من السلامة الشخصية والاجتماعية والأمنية لمستخدمى شبكة الإنترنت، كأن يتم إثبات هوية الشخص من خلال الكشف عن هوية الدولة.
- الشرطة التنبؤية: التى تقوم على العمل الاستباقى، بتبنى الأجهزة الشرطية لأنظمة التخزين السحابى لاستخدامها فى التنبؤ بالجرائم ومنع حدوثها، فمن شأن التخزين السحابى أن يجمع كما هائلا من البيانات ويحل مشاكل التخزين، ويتيح كذلك إمكانية ربط الشبكات الأمنية ببعضها.

تجدر الإشارة إلى أن استخدام تقنيات الذكاء الاصطناعي والتقنيات الحديثة وحدها لا تكفى للتنبؤ بالإرهاب الإلكتروني، مالم يتم رفع كفاءة الأجهزة الشرطية وتدريبهم على استخدام التقنيات التكنولوجية الحديثة، فالجرائم الإرهابية الإلكترونية آخذة فى النمو، وأنماط الجرائم قد أخذت صورا غير متوقعة، لذلك يجب على الأجهزة الشرطية اعتماد الذكاء الاصطناعي فى الاستراتيجية الأمنية لمكافحة الجرائم، وهو ما سوف نتناوله فى المطالب الآتية:

[1] انضمت مصر للاتفاقية بقرار رئيس الجمهورية رقم 276 لسنة 2014، بتاريخ 12/21/ 2010، وانضمت السعودية إلى الاتفاقية فى ذات التاريخ، بينما انضمت الأردن للاتفاقية بتاريخ 1/8/ 2013، والإمارات بتاريخ 9/21/ 2011.

[2] إبراهيم، على أحمد، مرجع سابق، ص 2824.

المطلب الأول: تطبيقات الذكاء الاصطناعي فى التنبؤ بالجرائم الإرهابية الإلكترونية

ترتكز تقنيات الذكاء الاصطناعي على تطوير الشبكات العصبية الصناعية التى تحاكى فى طريقة عملها العقل البشرى، بحيث تكون قادرة على التعلم والتجريب والقدرة على اتخاذ القرار بشكل منفصل عن الإنسان، الأمر الذى سمح لتقنيات الذكاء الاصطناعي باقتحام مختلف المجالات خصوصا المجال الأمني ومكافحة الجريمة، بحيث يتم توظيف خوارزميات الذكاء الاصطناعي من قبل الأجهزة الشرطية فى تحليل قواعد البيانات الخاصة بهم من أجل التنبؤ بالجرائم والمناطق الجغرافية التى قد يتوقع حدوثها بها[1].

فقد أحدث الذكاء الاصطناعي تحولا كبير فى مجال التنبؤ بالإرهاب الإلكتروني، حيث سمح لوكالات إنفاذ القانون بتحديد التهديدات المحتملة بسرعة كبيرة، باستخدام الشبكات العصبية للتنبؤ بالهجوم الإرهابي، بحيث تصل دقة الشبكةF1 العصبية إلى 0,954 أى 91 % من تلك التى تحققها نماذج القياسات البديلة، وإن كان استخدام الذكاء الاصطناعي للتنبؤ فى القرارات عالية المخاطر له قيود، بما فى ذلك التحيزات المحتملة والمخاوف الأخلاقية[2].

حيث يمكن لخوارزميات الذكاء الاصطناعي التنبؤ بالجرائم الإرهابية السيبرانية من خلال تحليل البيانات الوصفية لنظم الاتصالات والمعلومات، وكذلك للمعاملات المالية، ولمتصفح الإنترنت، وللمعلومات المتاحة عبر مواقع التواصل الاجتماعي، بينما تسمح أساليب التعلم الآلى من تفسير وتحليل الأنماط التى يصعب أو يتعذر الوصول إليها، وذلك من خلال تحليل أدوات أكثر تعقيدا للتعرف على الصوت أو الصورة، أضف إلى ذلك أن خوارزميات الذكاء الاصطناعي يمكنها التنبؤ بتوقيت الهجمات وأماكنها، فقد طورت بعض الشركات التكنولوجية من أدوات تقييم قابلية التعرض للأيديولوجيات المتطرفة مثل شركة "Jigsaw" التابعة لشركة "Alphabet Inc" التى أعلنت عن مشروع يعرف بإعادة التوجيه، حيث يستهدف مستخدمى المواقع الخاصة بمشاركة الفيديو، الذين قد يكونون عرضة للدعاية من قبل الجماعات الإرهابية كتنظيم داعش الإرهابي، بحيث يتم توجيه المستخدم حينئذ لمقاطع فيديو أخرى مضادة لرؤية التنظيم الإرهابي، كذلك يمكنها التعرف على الإرهابيين، حيث تم الاعتماد على خوارزمية معتمدة على الذكاء الاصطناعي من قبل وكالة الأمن القومى الأمريكى "SKYNET" لتحليل البيانات الوصفية ل 55 مليون مستخدم للهاتف المحمول فى باكستان، وتم اكتشاف أن حوالى 15 ألف فرد من إجمالى عدد السكان فى ذلك الوقت البالغ 200 مليون فرد هم إرهابيون محتملون[3].

فقد تغيرت فلسفة عمل أجهزة الشرطة من خلال الانتقال من التركيز على مقاضاة السلوك الإجرامي وأنشطة الإنفاذ إلى محاولة منع الجرائم من الأساس، وإلى التحول من جمع المعلومات عقب وقوع الحادث الإرهابي إلى محاولة منع وقوعه، فقد أصبحت الأجهزة الأمنية تتبنى اقترابات استباقية ترتكز على خطط طويلة الأمد، خاصة مع رغبة

[1] إبراهيم، على أحمد، مرجع سابق، ص 2810.

[2] Anna Rosner, Alexander Gegov, Djamila Ouelhadj, Adrian Alan Hopgood and Serge Da Deppo, Neural network based prediction of terrorist attacks using explainable artificial intelligence, paper in conference on Artificial Intelligence, United States, 2 August 2023.

[3] راشد، باسم، التنبؤ بالهجمات: فرص ومخاطر استخدامات الذكاء الاصطناعي فى مكافحة الإرهاب، سابق الإشارة إليه.

أجهزة إنفاذ القانون فى تبادل المعلومات الاستخباراتية حول العمليات الإرهابية والجرائم المنظمة[1]، حيث يمكن استخدام المعلومات الاستخباراتية فى الحد من تأثير المفاجأة الاستراتيجية الناجمة عن التهديدات الإجرامية[2].

فقد تفوقت خوارزميات الذكاء الاصطناعي والتقنيات التنبؤية الذكية (التنقيب عن البيانات– تقنية المتحكم الأصغر– التقنيات التنبؤية الجغرافية– تقنيات التعرف على الوجه) على الأساليب التقليدية للأجهزة الأمنية، فى الكشف عن السلوك الإرهابي، وكذلك فى رصد الأدلة الجنائية، حيث تتمكن الخوارزميات من تحليل البيانات والمعلومات فى وقت قصير وبسرعة عالية، مع ربطها ببعضها، تمهيدا للحصول على نتائج دقيقة تتفوق على التخمينات العشوائية التى تنتج عن الأساليب التقليدية، فهى توفر الإمكانيات اللازمة للتنبؤ بالسلوك الإجرامى، من خلال استخدام تقنيات التنقيب عن البيانات لاكتشاف المعرفة من قواعد البيانات[3].

فقد أصبح التنقيب عن البيانات والتحليلات التنبؤية جزءا لا يتجزأ من أعمال العديد من وكالات إنفاذ القانون، فالتحليلات التنبؤية تهدف إلى تحديد ما يمكن أن يحدث مستقبلا، من خلال تحليل البيانات المتوافرة، باستخدام الأساليب الإحصائية، بالإضافة إلى بعض الأساليب الأخرى التي تندرج تحت فئة التنقيب عن البيانات، ومن ثم اتخاذ الإجراءات الوقائية بناء على ذلك[4].

فيمكن الاستعانة بتقنية المتحكم الأصغر Micro–controller في المجال الأمني، من خلال القيام ببرمجة الوظائف الأمنية، تمهيدا لتنفيذها بمنتهى الدقة، مثل تطوير إدارة نظم المعلومات، أو نظم المعلومات الجغرافية، أو أي قواعد بيانات تتعلق بالأجهزة الأمنية، فالبيانات الضخمة Big Data يصعب التعامل معها دون استخدام هذه الخوارزميات المتطورة، من خلال هذه الإحصاءات الرياضية والمنطقية التي توفرها برامج تقنية المعلومات[5].

فيمكن لخوارزميات الذكاء الاصطناعي أن تراقب الملايين من تعليقات المستخدمين غير الهيكلية لفهم اتجاهاتهم، كما يمكن لتقنيات نظم المعلومات كبرامج نظم المعلومات الجغرافية GIS أن تسهم في توفير المحتوى بناء على النشاط والتركيبة السكانية عبر الإنترنت، ومن ثم اكتسبت العديد من مواقع الشبكات الاجتماعية أعمال الذكاء الاصطناعي، من خلال استخدام الذكاء الاصطناعي فى تحديد الخصائص الديموغرافية الجديدة، حيث تعتمد أدوات الذكاء الاصطناعي على خوارزميات التحليلات التنبؤية، التى تمكن من تجميع المعلومات عن نشاط كافة المستخدمين المعروفين في شبكة اجتماعية معينة لتقييم أو تحديد نشاط معين[6].

أضف إلى ذلك أن نظم المعلومات الجغرافية عندما يتم اقترانها بتقنيات أخرى، كأجهزة تحديد المواقع (GPS)، سوف تعمل على تحديد أماكن وجود الإرهابيين وتتبع تحركاتهم وتوزيعهم، ومعرفة خصائصهم الديموغرافية، فهذه

---

[1] البابلى، عمار ياسر محمد زهير، توظيف تقنيات الذكاء الاصطناعي فى العمل الأمنى، دراسة تطبيقية، مج 28، ع 1، مجلة الأمن والقانون، 2020، ص 31.

[2] John William Coyne & Peter Bell,The Role of Strategic Intelligence in Anticipating Transnational Organised pp. 60 . Vol. 39, Issue1, May 2011, Crime and Justice, International Journal of Law, Crime: A Literary Review,

[3] الأعرج، ماجد أحمد، مواجدة، مراد، بناء نموذج ذكاء اصطناعى لتعزيز الإجراءات الوقائية للحد من الجريمة فى المجتمع الأردنى، ع 44، المجلة العربية للنشر العلمى، 2 حزيران 2022، ص 101.

[4] عبدالحميد، كامل محمد فاروق، المعلومات الأمنية، أكاديمية نايف للعلوم الأمنية، الرياض، ط 1، 1999، ص 33.

[5] Grow-Hill, Jay. A .Farrell and Mathew .Barth .Jay, The Global Positioning System and Inertial Navigation, Mc New York, 2019, p 55-60.

[6] البابلى، عمار ياسر محمد زهير، توظيف تقنيات الذكاء الاصطناعي فى العمل الأمنى، مرجع سابق، ص 55.

النظم تعتبر أكثر فعالية من حيث التكلفة مقارنة بالتكلفة العالية التي تتكلفها دوريات ضباط الشرطة عند قيامها بالتتبع[1].

وتبرز أهمية نظم المعلومات الجغرافية في أنها ليست أداة لرسم الخرائط فحسب، بل تقنية فائقة الأداء تستخدم في تخزين البيانات الجغرافية وتوضيح المعلومات المكانية، من خلال تجميع البيانات وتخزينها وإمكانية تحديثها وتحليلها واسترجاعها ومعالجتها، والحصول على مخرجاتها، لإنشاء تمثيلات جديدة للمساحة الجغرافية، وتوفير أدوات التحليل المكانى، بشأن إجراءات التحليل الكمى والنوعى[2].

كما تستخدم نظم التعرف الآلي على الوجه كأحد تطبيقات الذكاء الاصطناعي، فى التحديد التلقائي أو للتحقق من وجود شخص ما في لقطة من مقطع فيديو أو فى صورة رقمية، وعادة ما يتم ذلك من خلال مقارنة ملامح الوجه المحدد وقاعدة بيانات الأجهزة الأمنية التى تحتوي على عدد كبير من الوجوه لأشخاص مختلفين، ومن ثم يتم استخدام أنظمة التعرف الآلي على الوجه في التطبيقات الأمنية على نطاق واسع[3].

فضلا عن استعانة الأجهزة الأمنية بالروبوتات فى حفظ الأمن والكشف عن الجرائم قبل وقوعها، من خلال التنبؤ بأماكن حدوثها بناء على الكشف عن أماكن وجود المجرمين وتتبعهم، وهو ما يندرج تحت استراتيجيات المدن الذكية التى تعتمد على استخدام التقنيات التكنولوجية فى حفظ الأمن والاستقرار وتحقيق الأهداف المستدامة[4].

المطلب الثانى: التحديات التى تواجه الخوارزميات الذكية فى مكافحة الجرائم الإرهابية الإلكترونية

هناك بعض التحديات التى يفرضها استخدام الدول للذكاء الاصطناعي فى التنبؤ بالجرائم الإرهابية الإلكترونية، خصوصا تقنيات الذكاء الاصطناعي القائمة على التعلم الآلى والتعلم العميق، التى يتم استخدامها فى تحديد الأفراد الذين يمثلون تهديدا للأمن القومى، فهذه التقنيات غالبا ما يتم استخدامها لتبرير اتخاذ مجموعة واسعة من التدابير الإدارية والأمنية التى قد تتعدى على الحقوق الأساسية للأفراد، كما أن هذه التقنيات غالبا ما يتم استخدامها دون وعى من عامة الناس[5].

أولا: التحديات المتعلقة بحقوق الإنسان: لا يوجد موقف دولى موحد حول حدود استخدام الذكاء الاصطناعي، الأمر الذى يمس حقوق الأفراد وحرياتهم، تلك الحقوق التى كفلها لهم الدستور والقانون، وهو ما يزيد الحاجة إلى وجود ضمانات كافية لاستخدام الذكاء الاصطناعي فى التنبؤ من قبل الحكومات والأجهزة الأمنية، ومراجعة التدابير الإدارية المتخذة من قبلهم، مع مراعاة خصوصية الأفراد وحرياتهم.

فعلى سبيل المثال: تكمن فائدة تقنية التعرف على الوجه في زيادة كفائتها ودقتها، حيث تعتمد على تطبيق النظام وقوة المعالجة، إلا أن تطور التكنولوجيا بشكل عام قد يتسبب في إشكاليات أخلاقية وقانونية، خاصة عندما يتم

---

[1] C-DAC, Pune University Campus, C.P. Johnson Geomatics Group, Crime Mapping and Analysis Using GIS, Translated by Mudar Khalil Omar, p.2.

[2] عبيد، حنان صبحى عبدالله ، الزيادى، حسين عليوى ناصر، الموسوى، محمد عرب نعمة، الاستراتيجيات المقترحة لتفعيل تقنية نظم المعلومات الجغرافية GIS في الحد من ظاهرتى الجريمة والإرهاب، مج 19، عدد خاص، مجلة ميسان للدراسات الأكاديمية، 2021، ص 11.

[3] البابلى، عمار ياسر محمد زهير، توظيف تقنيات الذكاء الاصطناعي فى العمل الأمنى، مرجع سابق، ص 65.

[4] الدسوقى، منى محمد العتريس، جرائم تقنيات الذكاء الاصطناعي والشخصية القانونية الإلكترونية المستقلة، دراسة مقارنة، العدد 81، مجلة البحوث القانونية والاقتصادية، سبتمبر 2022، 1146.

[5] Andrea Bianchi, Ann Greipl, States Prevention of Terrorism and the Rule of Law: Challenging the "magic" of Artificial Intelligence (AL), Op.Cit.

استخدام الصور الرقمية للأفراد دون موافقة أو تصريح الشخص المعنى، حيث يمكن تجميع البيانات وتوزيعها بدون معرفة الفرد، الأمر الذى ينطوى على انتهاك لخصوصية تلك البيانات[1].

وكذلك تستخدم تقنيات التعرف على الوجه فى التعرف على صور الأفراد، والتدخل فى خصوصية مستخدمى التواصل الاجتماعي من أجل معرفة اهتمامتهم، لاستخدامها من قبل الشركات فى الأغراض التجارية، وهو مايستلزم وضع ضوابط تنظيمية لوضع حد للصلاحيات الممنوحة لاستخدام الذكاء الاصطناعي لكى يبقى تحت السيطرة، كما يجب تسليط الضوء على خصوصية وسرية البيانات الشخصية للمستخدمين[2].

وقد ذكرت المفوضية الأوروبية فى هذا الصدد أنها تدرس حظر تقنية التعرف على الوجه في الأماكن العامة لمدة تصل إلى خمس سنوات، لكى تتمكن من وضع إطار تنظيمى، يُمكنها من منع التعدى وانتهاك خصوصية الأفراد[3].

ثانيا: العشوائية فى جمع البيانات: يعتمد المجال الأمني على جمع البيانات العشوائية لمختلف الأفراد، للقيام بعملية التنبؤ بالأنشطة الإرهابية أو غير القانونية.

ثالثا: التعتيم وعدم الشفافية المصاحبة لاستخدام الذكاء الاصطناعي فى التنبؤ بالجرائم الإرهابية الإلكترونية، أو فى استخدام البيانات المجمعة، مما يجعل من الصعب الحصول على ضمانات قانونية للشفافية فى مكافحة الإرهاب الإلكتروني.

رابعا: اقتصار جودة النماذج التنبؤية على الوصول للبيانات: حيث تقتصر جودة نماذج الذكاء الاصطناعي التنبؤى على القيود المفروضة على أنواع البيانات التى يمكن الوصول إليها.

خامسا: عدم التيقن من الحصول على نماذج تنبؤية دقيقة: نظرا للتعتيم وعدم الشفافية الذى يحيط استخدام الذكاء الاصطناعي التنبؤى فى مكافحة الإهاب الإلكتروني، حيث يجب التحقق من صحة النماذج واختبارها لقياس دقة التنبؤ.

سادسا: انخفاض معدل وقوع الهجمات الإرهابية وتطور أنماط الجرائم بسرعة كبيرة مع التطور التكنولوجى، يجعل من الصعب الحصول على نماذج تنبؤية دقيقة، خصوصا مع تقييد إمكانية الوصول إلى البيانات، الأمر الذى قد يؤثر على كفاءة خوارزميات الذكاء الاصطناعي فى تحليل البيانات.

سابعا: إساءة استخدام الذكاء الاصطناعي من قبل الحكومات لتحقيق الأغراض السياسية، من أجل فرض سيطرة شمولية على مواطنيها، الأمر الذى يستلزم تنظيم استخدام البيانات لإضفاء الرسمية على تحليل البيانات وتنظيم الشفافية.

ثامنا: تعميم تقنيات الذكاء الاصطناعي المستخدمه فى مواجهة الجرائم الإرهابية لمواجهة الجرائم الأخرى، على سبيل المثال: قامت إدارة شرطة مدينة نيويورك بدمج كاميرا Cctv3000 ، ANPR، إلى جانب أجهزة الاستشعار الأخرى المستخدمة خصيصا للتنبؤ بالعمليات الإرهابية، واستخدامها فى الأغراض العامة[4].

---

[1] Ian Berle, Face Recognition Technology Compulsory Visibility and Its Impact on Privacy and the Confidentiality of Personal Identifiable Images, Law, Governance and Technology Series, Volume 41, 2020, p.9.

[2] الدسوقى، منى محمد العتريس، مرجع سابق، ص 1146.

[3] Facial recognition: EU considers ban of up to five years, article in BBC News, 17 january 2020.

[4] راشد، باسم، التنبؤ بالهجمات: فرص ومخاطر استخدامات الذكاء الاصطناعي فى مكافحة الإرهاب، سابق الإشارة إليه.

وعلى الرغم من كافة هذه التحديات التى تواجه الذكاء الاصطناعي خلال مكافحته للإرهاب الإلكتروني، إلا أنه يمكن التغلب عليها من خلال الاستخدام المنظم لهذه التقنيات، الأمر الذى يعزز من قدرات الدول على حماية حقوق الأفراد وحرياتهم، ويحسن من الالتزام بالمبادئ التى تهدف إلى حماية الحقوق الأساسية لهم، مثل: مبدأ الشفافية والتناسب والتحرر من التمييز، كما يسهم أيضا فى الحماية من إساءة استخدام التكنولوجيات ذات الصلة[1].

الخاتمة

توصلت الدراسة إلى مجموعة من النتائج والتوصيات نبرزها فيما يلى:

النتائج

- يعد استخدام خوارزميات الذكاء الاصطناعي فى التنبؤ بالجرائم الإرهابية الإلكترونية جزءا من التحول من النهج التفاعلى إلى النهج الوقائى لمكافحة الإرهاب.
- يمكن للذكاء الاصطناعي وخوارزمياته التنبؤ بالإرهاب الإلكتروني بناء على البيانات الوصفية لنظم الاتصالات والمعلومات، والمعاملات المالية، وأنماط السفر، ونشاط تصفح الإنترنت، بالإضافة إلى المعلومات المتاحة للجمهور، فالتنبؤ الجيد أمر ضرورى لوضع استراتيجية لمكافحة الإرهاب الإلكتروني، دون التعدى غير المبرر على حقوق الأفراد.
- يقوم الذكاء الاصطناعي باستخدام الخوارزميات الرياضية فى القيام بعمليات حسابية واستنتاجية لتحقيق الأهداف الأمنية، من خلال استخدام تلك الخوارزميات فى معالجة البيانات الأمنية الرقمية، لمساعدة الأجهزة الرقمية فى وضع الخطوط العرضية لمواجهة الإرهاب الإلكتروني، عن طريق اكتشاف الاستباقات المعلوماتية واستنتاجها، وتحديد أماكن الجريمة والتنبؤ بوقوعها.
- يعد الذكاء الاصطناعي سلاحا ذا حدين، فكما يمكن استخدامه فى القيام بالهجمات السيبرانية، فإنه يمكن استخدامه أيضا فى التنبؤ بالجرائم الإرهابية الإلكترونية وقمعها، إلا أن استخدامها فى التنبؤ بالجرائم الإرهابية، قد يكون من شأنه أن يؤثر على الحقوق والحريات المدنية للأفراد، وإلى تفاقم العلاقة بين أفراد المجتمع ورجال إنفاذ القانون، وكذلك إلى التمييز العنصرى ضد جماعات أو طوائف معينة.
- وبتزايد انتشار استخدام الذكاء الاصطناعي من قبل أجهزة إنفاذ القانون، ازدادت أهمية وجود ضمانات أخلاقية، للتقليل من مخاطر انتهاك الحقوق الأساسية للإنسان، وضمان عدم إساءة استخدامها من قبل السلطة فى جمع الأدلة، من خلال الإشراف القضائي أو المستقل، مع مراعاة مبادئ الشرعية والضرورة والتناسب، كما ينبغى أن تمتثل الأدلة الإلكترونية للإجراءات المتعارف عليها حتى تكون مقبولة.
- تفوقت خوارزميات الذكاء الاصطناعي والتقنيات التنبؤية الذكية (التنقيب عن البيانات– تقنية المتحكم الأصغر– التقنيات التنبؤية الجغرافية– تقنيات التعرف على الوجه) على أساليب الأجهزة الأمنية التقليدية، فى الكشف عن السلوك الإرهابي الإلكتروني.

[1] Kathleen Mckendrick, Artificial Intelligence Prediction and counterterrorism, op.cit, p.3.

- يفرض استخدام الدول لتقنيات الذكاء الاصطناعي فى التنبؤ بالجرائم الإرهابية الإلكترونية بعض التحديات، فهذه التقنيات غالبا ما يتم استخدامها لتبرير اتخاذ مجموعة واسعة من التدابير الإدارية والأمنية التى قد تتعدى على الحقوق الأساسية للفرد، أضف إلى ذلك أن هذه التقنيات غالبا ما يتم استخدامها دون وعى من عامة الناس.

التوصيات

- ضرورة وجود ضمانات كافية (أخلاقية– فنية– تنظيمية) لاستخدام الذكاء الاصطناعي فى التنبؤ بالإرهاب الإلكتروني من قبل الحكومات والأجهزة الأمنية، ومراجعة التدابير الإدارية المتخذة من قبلهم، مع مراعاة خصوصية الأفراد وحرياتهم والامتثال للقواعد المتعلقة بحقوق الإنسان وحقهم فى الخصوصية.
- يجب أن تتم عمليات تحليل البيانات بشكل آلى، مع اتخاذ بعض التدابير الفنية للرقابة ومنع سوء استخدام تلك البيانات، بحيث يكون استمرار الوصول إلى البيانات لأغراض التنبؤ مشروطة بالقدرة على استخلاص قيمة تنبؤية من البيانات المحددة، مما يعنى تناسب إمكانية الوصول وارتباطه مباشرة بتحقيق أهدافا مشروعة.
- نوصى باستبدال التدابير الوقائية المستخدمة بضمانات فنية مثل سجلات التدقيق وتقييد الوصول المفروضة على الوصول للبيانات من قبل المستخدمين.
- ضرورة الاهتمام بإعداد خرائط أمنية رقمية لكافة المناطق، وكذلك إنشاء وحدات نظم معلوماتية وإشراك ذوى الخبرة فى اتخاذ القرارات الأمنية.

المراجع

المراجع العربية:

الرسائل العلمية

1. مخلف، مصطفى سعد حمد، جريمة الإرهاب عبر الوسائل الإلكترونية، دراسة مقارنة بين التشريعين الأردنى والعراقى، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، 2017.
2. الأبحاث القانونية
3. إبراهيم، على أحمد، تطبيقات الذكاء الاصطناعي فى مواجهة الجرائم الإلكترونية، مج 9، ع 8، المجلة القانونية، 2021.
4. أبو النجا، محمد عبدالحكيم محمد، دور االإستراتيجيات الأمنية لمواجهة جرائم الذكاء الاصطناعي وتكنولوجيا المعلومات، عدد خاص بالمؤتمر الدولى السنوى العشرون، مجلة البحوث القانونية والاقتصادية، 2021.
5. الأعرج، ماجد أحمد، مواجدة، مراد، بناء نموذج ذكاء اصطناعى لتعزيز الإجراءات الوقائية للحد من الجريمة فى المجتمع الأردنى، ع 44، المجلة العربية للنشر العلمى، 2 حزيران 2022.

6. البابلى، عمار ياسر محمد زهير، توظيف تقنيات الذكاء الاصطناعي فى العمل الأمني، دراسة تطبيقية، مج 28، ع 1، مجلة الأمن والقانون، 2020.
7. البابلى، عمار ياسر محمد زهير، دور أنظمة الذكاء الاصطناعي فى التنبؤ بالجريمة، مج 29، ع 1، مجلة الأمن والقانون، أكاديمية شرطة دبى، 2021.
8. البداينة، ذياب موسى، دور الأجهزة الأمنية فى مكافحة جرائم الإرهاب المعلوماتى، ورقة عمل مقدمة فى الدورة التدريبية بعنوان مكافحة الجرائم الإرهابية المعلوماتية فى الفترة من 9-13/4/ 2006، كلية التدريب، جامعة نايف العربية للعلوم الأمنية، المغرب، 2006.
9. الداغر، مجدى، اتجاهات النخبة نحو توظيف الإعلام الأمني لتطبيقات الذكاء الاصطناعي فى مكافحة الجرائم الإلكترونية وانعكاساته على دعم وتعزيز الأمن السيبرانى فى مصر، ع 33، المجلة العربية لبحوث الإعلام والاتصال، أبريل/يونيو 2021.
10. الدسوقى، منى محمد العتريس، جرائم تقنيات الذكاء الاصطناعي والشخصية القانونية الإلكترونية المستقلة، دراسة مقارنة، العدد 81، مجلة البحوث القانونية والاقتصادية، سبتمبر 2022.
11. دهشان، يحيى، المسئولية الجنائية عن جرائم الذكاء الاصطناعي، مج 34، ع 82، مجلة الشريعة والقانون، الإمارات، أبريل 2020.
12. راشد، باسم، التنبؤ بالهجمات: فرص ومخاطر استخدامات الذكاء الاصطناعي فى مكافحة الإرهاب، مركز المستقبل للأبحاث والدراسات المتقدمة، بتاريخ 9 أكتوبر 2019.
13. شادى عبد السلام، حروب الجيل الخامس، أساليب التفجير من الداخل على الساحة الدولية، مركز المستقبل للأبحاث والدراسات المتقدمة، الإمارات، 2020.
14. الشرايرى، محمد أحمد، المسئولية المدنية الذكية عن أضرار الذكاء الاصطناعي، دراسة مسحية مقارنة، ع2، ع تسلسلى 38، مجلة كلية القانون الكويتية العالمية، مارس 2022.
15. الشريف، محمود سلامة عبدالمنعم، الطبيعة القانونية للتنبؤ بالجريمة بواسطة الذكاء الاصطناعي ومشروعيته، مج 3، المجلة العربية لعلوم الأدلة الجنائية والطب الشرعى، 2021.
16. العامرى، سامر سعدون عبود، التحريض على ارتكاب الجرائم الإرهابية باستخدام وسائل التقنية الحديثة، ع 1، كلية القانون، جامعة بغداد، 2016.
17. عبدالحميد، كامل محمد فاروق، المعلومات الأمنية، ط1، أكاديمية نايف للعلوم الأمنية، الرياض، 1999.
18. عبيد، حنان صبحى عبدالله، الزيادى، حسين عليوى ناصر، الموسوى، محمد عرب نعمة، الاستراتيجيات المقترحة لتفعيل تقنية نظم المعلومات الجغرافية GIS في الحد من ظاهرتى الجريمة والإرهاب، مج 19، عدد خاص، مجلة ميسان للدراسات الأكاديمية، 2021.
19. محمود، رانيا سليمان أبو المعاطى، والدسوقى، نهى محمد إبراهيم، والصفتى، فاتن فايز حميدة، سياسة مكافحة الإرهاب الإلكتروني، مصر والسعودية أنموذجا، ع 53، المركز العربى للبحوث والدراسات، آفاق سياسية، 2020.

20.مرعى، أحمد لطفى السيد، انعكاسات تقنيات الذكاء الاصطناعي على نظرية المسئولية الجنائية، دراسة تأصيلية مقارنة، ع 80، مجلة البحوث القانونية والاقتصادية، يونيو 2022.
21.مصبح، عمر عبدالمجيد عبدالحميد، توظيف خوارزميات العدالة التنبؤية فى نظام العدالة الجنائية "الآفاق والتحديات"، مج 10، ع 1، المجلة الدولية للقانون، جامعة قطر، 2021.
22.ناجى، إسلام محروس، جرائم الإرهاب الإلكتروني، دراسة تأصيلية تحليلية للتشريع السعودى، ع 93، مجلة القانون والاقتصاد، كلية الحقوق، جامعة القاهرة، 2017.
23.نسيمة، مالك، عبدالنور، بعجى، الإرهاب الإلكتروني بين عولمة الجريمة وضرورة المكافحة، مج 7، ع 2، مجلة الدراسات والبحوث القانونية، كلية الحقوق، جامعة الجزائر، 2022.
24.ورقة معلومات أساسية أعدتها الأمانة العامة للأمم المتحدة بعنوان: التعاون الدولى وتقديم المساعدة التقنية من أجل منع الجرائم بجميع أشكالها والتصدى لها، مؤتمر الأمم المتحدة الرابع عشر لمنع الجريمة والعدالة الجنائية، كيوتو، اليابان، 20–27 أبريل 2020.

القوانين واللوائح

1. قانون حماية البيانات الشخصية المصرى رقم 151 لسنة 2020.
2. قانون حماية البيانات الشخصية الإتحادى رقم 45 لسنة 2021، المنشور فى الجريدة الرسمية العدد 712 (ملحق 1)، بتاريخ 2021/09/26.
3. اللائحة التنظيمية الأوروبية رقم 967/ 2016، الصادرة عن البرلمان والمجلس الأوروبى فى27 أبريل 2016، التى ألغت التوجيه 46/95، ودخلت حيز التنفيذ في 25 ماى 2018.

المراجع الأجنبية

1. ACLU, "Statement of Concern About Predictive Policing by ACLU and 16 Civil Rights Privacy, Racial Justice, and Technology Organizations", August 31 2016, available at: https://www.aclu.org/other/statement-concern-about-predictive-policing-aclu-and-16-civil-rights-privacy-racial-justice .
2. Andrea Bianchi, Ann Greipl, States Prevention of Terrorism and the Rule of Law: Challenging the “magic” of Artificial Intelligence (AL) Article at ICCT, 17 Nov 2022, available at: https://www.icct.nl/publication/states-prevention-terrorism-and-rule-law-challenging-magic-artificial-intelligence-ai.
3. Anna Rosner, Alexander Gegov, Djamila Ouelhadj, Adrian Alan Hopgood and Serge Da Deppo, Neural network based prediction of terrorist attacks using explainable artificial intelligence, paper in conference on Artificial Intelligence, United States, 2 August 2023.
4. C.P. Johnson Geomatics Group, Crime Mapping and Analysis Using GIS, C-DAC, Pune University Campus, Translated by Mudar Khalil Omar, p.2.
5. Facial recognition: EU considers ban of up to five years, article in BBC News, 17 january 2020.

6. Ian Berle, Face Recognition Technology Compulsory Visibility and Its Impact on Privacy and the Confidentiality of Personal Identifiable Images, Law, Governance and Technology Series, Volume 41, 2020, p.9.
7. Jay. A .Farrell and Mathew .Barth .Jay, The Global Positioning System and Inertial Navigation, Mc Grow-Hill, New York, 2019.
8. John William Coyne & Peter Bell, The Role of Strategic Intelligence in Anticipating Transnational Organised Crime: A Literary Review, International Journal of Law, Crime and Justice, Vol. 39, Issue1, May 2011.
9. Judith Rochfeld, L'encadrement des décisions prises par les algorithmes, Dalloz IP/IT, n°9, 2018.
10. Kathleen Mckendrick, Artificial Intelligence Prediction and counterterrorism, International Security Department, August 2019.
11. Tanya Mehra, Matthew Wentworth, and Bibi Van Ginkel, The Expanding Use of Administrative Measures in a Counter-Terrorism Context- Part 1: In Need of Rule of Law Safeguards, Article in ICCT, 10 Nov 2021, available at: https://www.icct.nl/publication/states-prevention-terrorism-and-rule-law-challenging-magic-artificial-intelligence-ai.