PERDANA
INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH
eISSN: 2600-9463

# THE ROLE OF ARTIFICIAL INTELLIGENCE IN COMBATING THE CRIME OF ELECTRONIC TERRORIST FINANCING

# دور الذكاء الاصطناعي في مكافحة جريمة تمويل الإرهاب الإلكتروني

Mohammed Khalifa Mohammed Suliman Al Hanaee [1] & Nisar Mohammad Ahmad[2]

[1] PhD Student, Faculty of Syariah and Law, Universiti Sains Islam Malaysia (USIM). mohd.khalifa@hotmail.com
[2] Associate Professor, Faculty of Syariah and Law, Universiti Sains Islam Malaysia (USIM). nisar@usim.edu.my

**Vol. 19. No. 1**
**April Issue**
**2024**

**Abstract**

*This research aims to recognise the crime of cyber terrorism and its financing, as well as the methods of combating this crime using artificial intelligence (AI). The study also sheds light on the efforts made in the United Arab Emirates (UAE) in this context and the role of legislation in this regard. The descriptive analytical approach was adopted in this study, where the nature of cyber terrorism and its sources of financing were substantive and the provisions of the UAE's current legislation on combating currency laundering and terrorist financing were analyzed. Moreover, the study depicts the role played by AI and the applications it uses in struggling with and countering cyberterrorism financing. The study reached a set of recommendations, the most serious of which are the following: (1) Growing interest in AI and its development in combating crimes. (2) It is necessary to set up a legal and ethical framework to govern the use of AI technologies. (3) The diffuse trend is to realise terrorist financing as an independent criminal model, in spite of its link to other crimes.*

Keywords: *Terrorism, Cyber, Artificial Intelligence, Legislation, UAE.*

**ملخص البحث**

يهدف البحث إلى التعرف على جريمة الإرهاب الإلكتروني وتمويله وطرق مكافحة هذه الجريمة عن طريق الذكاء الاصطناعي، وإلقاء الضوء على الجهود المبذولة في دولة الإمارات العربية المتحدة في هذا الإطار ودور التشريع في ذلك، واعتمدت هذه الدراسة على المنهج الوصفي التحليلي؛ حيث تم وصف طبيعة الإرهاب الإلكتروني ومصادر تمويله، وتحليل أحكام التشريعات الإماراتية النافذة في مجال مكافحة غسل الأموال وتمويل الإرهاب، بالإضافة إلى وصف الدور الذي يلعبه الذكاء الاصطناعي والتطبيقات التي يستخدمها في مكافحة تمويل الإرهاب الإلكتروني ومواجهته. وتوصَّلت الدراسة إلى مجموعة من النتائج والتوصيات من أهمها ما يلي: (١) الاهتمام المتزايد بالذكاء

الاصطناعي وتطويره في مكافحة الجرائم. (٢) لا بد من إنشاء منظومة قانونية وأخلاقية تحكم عملية الاستعانة بتقنيات الذكاء الاصطناعي. (٣) الاتجاه الغالب يميل نحو تعريف تمويل الإرهاب بوصفه نموذجًا "إجراميًّا" مستقلًا على الرغم من الربط بينه وبين جرائم أخرى.

الكلمات المفتاحية: الإرهاب، الإلكتروني، الذكاء الاصطناعي، التشريع، الإماراتي.

**مقدمة**

ظاهرة الفضاء السيبراني هي من سمات الثورة التكنولوجية، كما أن لها دورًا استراتيجيًّا في الأبعاد الاقتصادية والسياسية والثقافية والأمنية والاجتماعية للمجتمع الدولي، فمع بداية الموجة العالمية للانتشار التكنولوجي وتزايد الاهتمام بمجال الاتصالات وتكنولوجيا المعلومات كوسيلة مهمة لتحقيق النمو الاقتصادي السريع، ظهرت تهديدات عديدة للاستخدام السلبي للبيانات من هذه التقنيات، مثل استخدام هذه البيانات في تنفيذ العمليات الإرهابية، وظهور المصطلحات التي تصف الأنشطة غير المناسبة في الفضاء السيبراني بطريقة تؤثر على طبيعتها ودورها، وبالتالي أهميتها الاستراتيجية في النظام الدولي. وفي هذا السياق، يبرز مفهوم الإرهاب الإلكتروني كأحد التحديات الرئيسة.

أظهرت العديد من الدراسات التي تناولت ظاهرة الإرهاب أن النشاط الإرهابي قد انتقل إلى الفضاء الإلكتروني بعد أحداث سبتمبر ٢٠٠١، وبينما كان الإرهابي يستخدم في الماضي الأسلحة التقليدية مثل: البنادق والقنابل، فإنه اليوم مسلح بجهاز كمبيوتر محمول وكاميرا، هذا ما أكده جودت هوشيار، الذي أشار إلى أن استراتيجية داعش الإعلامية تعتمد على استغلال الإنترنت والشبكات الاجتماعية والهواتف الذكية للوصول إلى الناس وتنسيق الإرهابيين على مختلف المستويات (هوشيار، ٢٠١٤).

استخدمت الجماعات الإرهابية التكنولوجيا كأداة رئيسة لتحقيق أهدافها وأصبحت جزءًا لا يتجزأ من اللوجستيات الداعمة والمستضيفة لأنشطتها الإعلامية في مناطق مختلفة من العالم، وباستخدام الإنترنت يمكن لهذه الجماعات تصوير أنشطتها ونشرها بالسياق والضوء الذي يخدم أغراضها بدون تدخل وسائل الإعلام الرسمية ودون تعريض صورتها للتحريف أو التغيير، لقد بدأ الإرهابيون في استخدام الفضاء الإلكتروني للتأثير على الرأي العام، وجذب المزيد من الأعضاء وجمع الأموال (الجخة وعادل، ٢٠٠٩).

وخلال السنوات الأخيرة، قفز التطور في تقنية الذكاء الاصطناعي قفزات كبيرة، وتعد تقنية "التعلم العميق" أبرز مظاهره، والتي ترتكز على تطوير شبكات عصبية صناعية تحاكي في طريقة عملها أسلوب الدماغ البشري، أي أنها قادرة على التجريب والتعلم وتطوير نفسها ذاتيًّا دون تدخل، وهذا يدل على دور الذكاء الاصطناعي الأساسي في مختلف مجالات العلم وبخاصة في مجال مكافحة الإرهاب. ولقد بذلت دولة الإمارات

العربية المتحدة –كغيرها من الدول– جهودًا كبيرة لمواجهة تمويل الإرهاب ومكافحة غسل الأموال والجرائم المالية. وتهدف سياسات وقوانين دولة الإمارات العربية المتحدة إلى اكتشاف ومنع الجرائم المالية، ولا يُسمح بارتكاب أية جرائم مالية على أراضيها أو استخدامها كوسيلة لتحويل الأموال الناتجة عن أي نشاط إجرامي، وتدعم الدولة الإماراتية الجهود العالمية لمكافحة غسل الأموال وتمويل الإرهاب.

## مشكلة البحث

تكمن مشكلة الدراسة في حداثة الموضوع وخطورة من يقوم بهذا النوع من الجرائم، فضلًا عما يحتاجه القضاء على هذه الجرائم من متطلبات قانونية وتقنية متميزة، وبناء على هذه المشكلة نطرح التساؤلات التالية:

## تساؤلات البحث

تطرح هذه الدراسة تساؤلاً رئيسًا هو: كيف يتم تمويل الإرهاب الإلكتروني؟ وما الأدوار والمهام التي يقوم بها الذكاء الاصطناعي لمواجهته؟ يتبع هذا السؤال عِدة أسئلة فرعية:

١. ما جريمة الإرهاب الإلكتروني وتمويله؟
٢. ما وسائل الإرهاب الالكتروني؟ وما طرق تمويله؟
٣. كيف تُواجَه جرائم الإرهاب حسب التشريع الإماراتي؟
٤. ما المقصود بالذكاء الاصطناعي؟

## أهداف البحث

تهدف الدراسة إلى ما يلي:

١. معرفة جريمة الإرهاب الإلكتروني وتمويله.
٢. معرفة وسائل الإرهاب الإلكتروني وطرق تمويله.
٣. إبراز أهم الجهود لمكافحة الإرهاب وتمويله في الإمارات العربية المتحدة.
٤. معرفة ماهية الذكاء الاصطناعي وطرقه في مواجهة الإرهاب الإلكتروني.

## أهمية البحث

تتمثل أهمية الدراسة في أنها تُبرز جريمة لا يمكن التغاضي عنها ألا وهي جريمة الإرهاب الإلكتروني وتمويله، والوسائل المتخذَة لذلك، ومواجهته في التنظيم الإماراتي. بالإضافة إلى تسليط الضوء على تطبيقات الذكاء الاصطناعي والدور الذي تقوم به في مكافحة هذا النوع من الجرائم.

**حدود البحث**

١. الحدود الموضوعية: يتناول البحث موضوع تمويل الإرهاب الإلكتروني، ودور الذكاء الاصطناعي في مواجهته وفقًا للتشريع الإماراتي طبقًا للمرسوم بقانون اتحادي رقم (٢٠) لسنة ٢٠١٨ في شأن "مواجهة جرائم غسل الأموال ومكافحة تمويل الإرهاب وتمويل التنظيمات غير المشروعة"، وقرار مجلس الوزراء رقم (١٠) لسنة ٢٠١٩ في شأن "اللائحة التنفيذية للمرسوم" بقانون اتحادي رقم (٢٠) لسنة ٢٠١٨ في شأن "مواجهة جرائم غسل الأموال ومكافحة تمويل الإرهاب وتمويل التنظيمات غير المشروعة".

٢. الحدود الزمانية: ينحصر البحث في موضوع تمويل الإرهاب الإلكتروني، ودور الذكاء الاصطناعي في مواجهته وفقًا للتشريع الإماراتي لمرسوم بقانون اتحادي رقم ٢٠ لسنة ٢٠١٨ في شأن "مواجهة جرائم غسل الأموال ومكافحة تمويل الإرهاب وتمويل التنظيمات غير المشروعة"، قرار مجلس الوزراء رقم (١٠) لسنة ٢٠١٩ في شأن "اللائحة التنفيذية للمرسوم" بقانون اتحادي رقم (٢٠) لسنة ٢٠١٨ بشأن "مواجهة جرائم غسل الأموال ومكافحة تمويل الإرهاب وتمويل التنظيمات غير المشروعة".

٣. الحدود المكانية: يتناول البحث موضوع تمويل الإرهاب الإلكتروني، ودور الذكاء الاصطناعي في مواجهته وفقًا للتشريح الإماراتي، وعليه تنحصر الحدود المكانية في إطار دولة الإمارات العربية المتحدة وأية جرائم تواجهها من الخارج.

**منهج البحث**

اعتمدت هذه الدراسة على المنهج الوصفي التحليلي؛ حيث تم وصف طبيعة الإرهاب الإلكتروني ومصادر تمويله، بالإضافة إلى وصف الدور الذي يلعبه الذكاء الاصطناعي والتطبيقات التي يستخدمها في مكافحة تمويل الإرهاب الإلكتروني ومواجهته.

**المبحث الأول: مفهوم الإرهاب الإلكتروني وأساليبه وسياسات مكافحته حسب التشريع الإماراتي**

لقد سبقت الشريعة الإسلامية الغرَّاء –في هذا الصدد– القوانين الوضعية في تحريم الاعتداء على النفس البشرية وأموال الناس؛ حيث اعتبرت النفوس كلها واحدة ومَن اعتدى على إحداها كأنما اعتدى عليها جميعًا، وهو ما يدفعنا للقول إن الإسلام يحارب الإرهاب بشتى صوره وأنواعه، فهو في الأساس دين السلام، فمبدأ السلام في ديننا الحنيف أعمق من أن يكون مجرد غاية يرمي إلى تحقيقها في الحياة، بل هو أصل من أصول عقيدته، وعنصر من عناصر تربيته، وهدف يعمّق الإحساس به في ضمير الفرد وواقع المجتمع، وجسد الأمة (رمضان، ٢٠١٦: ١١٠٧)

وقد عرَّف مجمع البحوث الإسلامية بالأزهر الإرهاب بعد أحداث الحادي عشر من سبتمبر ٢٠٠١م بأنه: "هو ترويع الآمنين وتدمير مصالحهم ومقومات حياتهم والاعتداء على أموالهم وأعراضهم وحرياتهم

وكرامتهم الإنسانية بغيًا وإفسادًا في الأرض. ومن حق الدولة التي يقع على أرضها هذا الإرهاب الأثيم أن تبحث عن المجرمين وأن تُقدمهم للهيئات القضائية لكي تقول كلمتها العادلة فيهم" (الأحمد، د.ت: ١٤١).

ويواجه العديد من الأكاديميين والخبراء والمحللين تحديًا عند تعريف الإرهاب، ولم يقتصر الأمر على الأفراد فقط، بل واجه المجتمع الدولي نفس التحدي أيضًا، وحتى الآن لا يزال العمل على وضع تعريف شامل ومتفَق عليه للإرهاب على المستوى الدولي أمرًا يواجه الصعوبات؛ بسبب تعقيد ظاهرة الإرهاب وتغيُّر أنماطها المتكررة، وكثيرًا ما تختلط بظواهر أخرى مثل: الجريمة المنظَّمة والعنف السياسي والنزاعات المسلحة، مما يجعل من الصعب معرفة حدود هذه الظاهرة ومكافحتها (راشد، ٢٠٠٦).

وعلى ضوء ما تقدم يسعى هذا المبحث إلى التعرف على مفهوم الإرهاب الإلكتروني وأساليب تمويله وسياسات المشروع الإماراتي في مكافحته وفق مطلبين:

## المطلب الأول: مفهوم الإرهاب الإلكتروني وأساليبه

### مفهوم الإرهاب الالكتروني:

رغم وجود تعاريف مختلفة للإرهاب، إلا أنه لا يوجد تعريف شامل ومحدد لهذا المفهوم على المستوى الدولي. ومن بين هذه التعاريف، تعريف الموسوعة السياسية الذي يصف الإرهاب على أنه: "استخدام العنف غير القانوني أو التهديد به لتحقيق أهداف سياسية، ويشمل ذلك الاغتيال والتشويه والتعذيب والتخريب والنسف؛ بغية إخضاع الآخرين لمشيئة الجهة الإرهابية أو الحصول على المال أو المعلومات. يتم استخدام الإرهاب عموما كوسيلة لكسر الروح والالتزام عند الأفراد وتدمير المعنويات عند المؤسسات والهيئات" (الكيالي، ١٩٩٤).

كما أنه لا يوجد تعريف شامل جامع لمفهوم الإرهاب الإلكتروني، ويندرج ضمن مفهوم الإرهاب العام؛ إذ ظهرت فكرة الإرهاب الإلكتروني Cyber terrorism في الثمانينيات من القرن العشرين، وعرَّفه باري كولين Barry Collin بأنه: "هجوم إلكتروني يهدف إلى تهديد الحكومات أو الاعتداء عليها بهدف تحقيق أهداف سياسية أو دينية أو أيديولوجية، ويجب أن يكون ذا تأثير مدمر وتخريبي مكافئ لأفعال الإرهاب الجسدية (الصادق، ٢٠٠٩).

كما يصف (دورثي دينينغ) الإرهاب الإلكتروني على أنه: "اعتداء يستهدف الأجهزة الحاسوبية، ويهدف التهديد به إلى إرهاب الحكومات أو المجتمعات لتحقيق أهداف سياسية أو دينية أو فكرية، ويتميز بالتدمير والتخريب الشامل لتحقيق الخوف والذعر على نحو يشبه الأعمال الإرهابية الفعلية (Denning, 2000).

يُعرَّف الإرهاب الإلكتروني بشكل إجرائي بأنه: نشاط أو هجوم متعمَّد، يهدف إلى التأثير على القرارات الحكومية أو الرأي العام، ويستخدم الفضاء الإلكتروني كعامل مساعد ووسيط في عملية تنفيذ

الأعمال الإرهابية أو الحربية، ويتم ذلك من خلال هجمات مباشرة باستخدام القوة المسلحة على مقدرات البنية التحتية للمعلومات، أو عن طريق التحريض على بث الكراهية الدينية وحرب الأفكار، أو باستخدام آليات الأسلحة الإلكترونية الجديدة في معارك تدور في الفضاء الإلكتروني، والتي يمكن أن يقتصر تأثيرها على الأبعاد الرقمية أو تتعدى ذلك لتصيب أهدافًا مادية تتعلق بالبنية التحتية الحيوية، وينطوي الإرهاب الإلكتروني أيضًا على تأثيرات نفسية ومعنوية (الصادق، ٢٠٠٧).

يعتمد الإرهاب الإلكتروني على الأساليب التكنولوجية الحديثة، وتتضمن هذه الأساليب استخدام الإمكانيات التقنية المتاحة وتحديدًا شبكات المعلوماتية، بهدف ترويع الأفراد وتهديدهم وإلحاق الضرر الفعلي بهم (دودح، ٢٠١٦).

## أساليب وأهداف الإرهاب الإلكتروني

يُعدُّ استخدام الجماعات الإرهابية للفضاء الإلكتروني كوسيلة لارتكاب الإرهاب السيبراني أخطر أشكال الإرهاب وأحدثها، ويقوم على استخدام شبكة الإنترنت وشبكات المعلومات وأجهزة الكمبيوتر وما يرتبط بها من تطورات تكنولوجية متسارعة من أجل التخويف والإرغام والتخريب لتحقيق أهداف سياسية. ويمثل الإرهاب الإلكتروني أحد مظاهر الدمج والربط بين استخدام العنف لتحقيق أهداف سياسية، وتوظيف التكنولوجيا الحديثة في مجالات الاتصال والمعلوماتية، والتي تُعدُّ من أبرز آليات العولمة وهي موجهة إلى (الصادق، ٢٠٠٩): النظم العسكرية، والبنية التحتية الاقتصادية، ومحطات توليد الطاقة والماء، ونظم الاتصالات، ونظم المواصلات" (Dogrul et al., 2011)، ويمكن بلورة وسائل استخدام الجماعات الإرهابية للفضاء الإلكتروني على النحو الآتي:

١. التنسيق والاتصال: تستخدم الجماعات الإرهابية التكنولوجيا الحديثة لتنظيم وتخطيط عملياتها، وذلك عن طريق استخدام البريد الإلكتروني والمواقع الإلكترونية ووسائل التواصل الاجتماعي؛ لتجنب المخاطر المرتبطة بالاجتماعات المباشرة، كما أن استخدام هذه الوسائل يصعب تتبعها (خاطر و حسن، ٢٠١٥).
٢. الترويج الإعلامي: يستخدم بعض الأشخاص وسائل التواصل الاجتماعي لنشر بياناتهم الخاصة والترويج لأيديولوجياتهم، كما ينشرون الأخبار الزائفة والشائعات لتحريض الآخرين على العنف والإرهاب والفتنة (مكتب الأمم المتحدة المعني بالمخدرات والجريمة، ٢٠١٣).
٣. التجسس على المواقع وتدميرها: تقوم فئة متخصصة من المبرمجين بالاختراق غير القانوني للمواقع الإلكترونية والشبكات، ويكون هذا بهدف تدمير البنية التحتية المعلوماتية للجهات الحكومية والخاصة، أو للحصول على معلومات تخص مؤسسات مهمة (Weimann, 2006).

**٤.** الحرب الدعائية: تهدف إلى جذب عدد كبير من الأفراد، وخاصة القُصَّرَ، وتجنيدهم للمساهمة في تحقيق هدفين رئيسين، الهدف الأول: هو جذب الأفراد للمشاركة في هذه الأهداف، بينما الهدف الثاني: هو الحصول على الدعم والموارد المالية اللازمة لتحقيق هذه الأهداف (خاطر و حسن، ٢٠١٥).

**المطلب الثاني: سياسات دولة الإمارات العربية المتحدة في مكافحة الإرهاب الإلكتروني**

لقد اتخذت دولة الإمارات حزمة من الإجراءات لمكافحة جريمة تمويل الإرهاب الإلكتروني، فقد صادقت على العديد من الاتفاقيات الدولية، وسنَّت التشريعات، وأنشأت مكتبًا تنفيذيًّا، ونفَّذت ممثَّلة في هيئة تنظيم الاتصالات والحكومة الرقمية شبكة اتحادية معزَّزة ببنية تحتية مشتركة (FedNet) تسمح بالتوصيل البيني، وتبادل البيانات بين جميع الجهات المحلية والاتحادية في الدولة، وتعزز قنوات التواصل فيما بينها باستخدام بنية تكنولوجية موحَّدة وآمنة، إلى جانب العديد من الجهود الدولية والمحلية لمكافحة هذه الجريمة (البوابة الرسمية لحكومة الإمارات العربية المتحدة، ٢٠٢٣).

وقد بلغت القيمة الإجمالية لعمليات وإجراءات مواجهة غسل الأموال ومكافحة تمويل الإرهاب خلال العام ٢٠٢١، بما يقدر بنحو ١,٠٤٨ مليار دولار –٣,٨٤٨ مليار درهم– حسب بيانات المكتب التنفيذي لمواجهة غسل الأموال وتمويل الإرهاب في دولة الإمارات العربية المتحدة (وكالة أنباء الإمارات، ٢٠٢٢).

وعلى المستوى التشريعي، تم إجراء عدد من التعديلات القانونية الرئيسة خلال الفترة الماضية مثل التعديل الخاص بقانون غسل الأموال ليتضمن صلاحيات أوسع بشأن المصادرات، بالإضافة إلى وضع ضوابط للأصول الافتراضية والتي تُعدُّ من أهم التعديلات على مستوى المنطقة، مشيرًا إلى أنه يتم حاليًا العمل على إصدار تعديل للائحة التنفيذية لقانون مواجهة غسل الأموال، علاوة على التعديلات الخاصة بنظام الإدراج في قوائم مجلس الأمن؛ وذلك لمكافحة تمويل الإرهاب وتعزيز منظومة العقوبات المالية المستهدفة (جريدة الاتحاد، ٢٠٢٢).

واعتمد المشرع الإماراتي نظامًا لتعريف تمويل الإرهاب وتعريفًا آخَر لتمويل المنظمات غير المشروعة، وذلك بموجب المرسوم الاتحادي للقانون رقم ٢٠ لعام ٢٠١٨، فبموجب هذا المرسوم، يتم تعريف "تمويل الإرهاب" على أنه: "أي فِعل من الأفعال المحددة في المادتين ٢٩ و٣٠ من القانون الاتحادي رقم ٧ لعام ٢٠١٤ المتعلق بمكافحة الجرائم الإرهابية (المادتين [٢٩–٣٠]، ٢٠١٤).

ويتضح من هاتين المادتين أن المشرع الإماراتي قد ساوى بين كل صور الإمداد بالأموال، كما ورد تعريفها في القانون، بشرط أن تقدم أو يتم جمعها أو تأمين الحصول عليها، لمن ينطبق عليهم قانون مكافحة الجرائم الإرهابية، سواء كانوا أفرادًا عاديين أو تنظيمات، أيًّا كان شكلها أو المسمَّى الخاص بها، وسواء كانت داخل الدولة أو خارجها. كما يتضح من التعريف السابق مدى الربط بين غسل الأموال وتمويل الإرهاب

على صعيد التجريم والعقاب؛ حيث تتقارب بشكل كبير أركان الجريمتين بما يمكن اعتبارهما نموذجًا إجراميًّا واحدًا، خاصة ما ورد في المادة (٣٠) من القانون الاتحادي رقم ٧ لسنة ٢٠١٤ (المادة [٣٠]، ٢٠١٤).

وضع المشرع الإماراتي تعريفًا لتمويل التنظيمات الإرهابية، يشمل أي فعل أو تصرف مادي يهدف إلى توفير الأموال لتنظيم غير مشروع، أو لأحد أنشطته، أو لأحد أفراده، ومن ثَمَّ فقد ساوى في تمويل التنظيمات غير المشروعة بين التنظيم ذاته وأنشطته والمنتمين إليه، كما ساوى بين الفعل المادي، مثل: القيام بدفع أو تحويل أموال، وبين التصرف القانوني مثل: البيع أو الهبة أو الايجار ... إلخ، طالما كان المراد منها توفير المال لتلك التنظيمات أو أنشطتها أو أحد المنتمين إليها، بما يضمن الإحاطة بجميع صور وأشكال التمويل الموجهة للتنظيمات غير المشروعة، والتي لا يُشترط أن تكون منخرطة في أعمال الإرهاب، أو على صلة بأحد الإرهابيين أو الجماعات الإرهابية، وقد حددها المشرع في القانون ذاته بأنها "التنظيمات المجرَّم إنشاؤها أو أحد أنشطتها"، بل إن المرسوم بقانون اتحادي رقم (٢٠) لسنة ٢٠١٨، أورد في المادة (٣) منه نموذجًا تجريميًّا لتمويل الإرهاب وتمويل التنظيمات غير المشروعة (المادة رقم [٣]، ٢٠١٨).

وأيقنت العديد من الدول العربية أهمية الربط في التجريم والعقاب وأساليب المكافحة، وبين غسل الأموال وتمويل الإرهاب باعتبارهما ظاهرتين إجراميتين يصعب الفصل بينهما، ولذلك قامت بالعديد من الجهود التي تعكس الاهتمام الكبير الذي توليه لمكافحتهما بتعديل تشريعاتها الجنائية المتعلقة بمكافحة غسل الأموال لتضم إليها مكافحة تمويل الإرهاب، بعد تصديق الدول العربية على الاتفاقية العربية لمكافحة غسل الأموال وتمويل الإرهاب في عام ٢٠١٠، تعزز هذا الاتجاه التشريعي العربي وتمثل الاتفاقية إدراكًا حقيقيًا من جانب الدول العربية لمخاطر العلاقة بين غسل الأموال وتمويل الإرهاب؛ فهذه المخاطر تقوض خطط التنمية الاقتصادية وتعرقل جهود الاستثمار في الدول العربية، مما يهدد الاستقرار السياسي والاقتصادي والأمني ويخل بسيادة القانون في تلك الدول (مويس، ٢٠٢٠).

صادقت دولة الإمارات العربية المتحدة على اتفاقية مكافحة غسل الأموال وتمويل الإرهاب بالمرسوم الاتحادي رقم (٦٨) لسنة ٢٠١١ في السادس من يوليو من نفس العام، وعلى إثر ذلك تم تعديل قانون تجريم غسل الأموال رقم (٤) لسنة ٢٠٠٢ ليحل محله القانون الاتحادي رقم (٤) لسنة ٢٠٠٢ بشأن مواجهة جرائم غسل الأموال ومكافحة تمويل الإرهاب، وذلك بمقتضى الفقرة الأولى من المادة الأولى من القانون الاتحادي رقم (٩) لسنة ٢٠١٤. ولم يكتفِ المشرع الإماراتي بتلك التعديلات الجزئية؛ إذ تم إلغاء القانون الاتحادي رقم (٩) لسنة ٢٠١٤ بموجب المرسوم بقانون اتحادي رقم (٢٠) لسنة ٢٠١٨، بشأن مواجهة جرائم غسل الأموال ومكافحة تمويل الإرهاب وتمويل التنظيمات غير المشروعة، حيث جمعت الجرائم الثلاثة في قانون واحد.

يمكن القول إن الجانب القانوني في دولة الإمارات يتضمن إصدار قوانين وتشريعات لمكافحة الإرهاب، حيث تم تجريم أية عناصر ترتبط بالتنظيمات الإرهابية، ومن بين هذه القوانين:

١. القانون الاتحادي رقم (٧) لسنة ٢٠١٤ في شأن مكافحة الجرائم الإرهابية.
٢. مرسوم بقانون اتحادي رقم (٢) لسنة ٢٠١٥ في شأن مكافحة التمييز والكراهية.
٣. مرسوم بقانون اتحادي رقم (٥) لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات.
٤. المرسوم بقانون اتحادي رقم (٢٠) لسنة ٢٠١٨ في شأن مواجهة جرائم غسل الأموال ومكافحة تمويل الإرهاب وتمويل التنظيمات غير المشروعة ولائحته التنفيذية.
٥. إصدار قائمة محلية بالكيانات الإرهابية وجاء ذلك تطبيقًا لأحكام القانون الاتحادي رقم (٧) لسنة ٢٠١٤ بشأن مكافحة الإرهاب.

**إنشاء دائرة مواجهة غسل الأموال ومكافحة تمويل الإرهاب**

أسّس مصرف الإمارات العربية المتحدة المركزي دائرة مخصّصة لمعالجة كافة الأمور المتعلقة بمواجهة غسل الأموال ومكافحة تمويل الإرهاب (AML/CFT).

تتركّز مهام وأعمال "دائرة الإشراف على مواجهة غسل الأموال ومكافحة تمويل الإرهاب" في تحقيق ثلاثة أهداف رئيسة هي (وزراة الخارجية والتعاون الدولي، ٢٠٢١):

١. إجراء عمليات التفتيش على المؤسسات المالية المرخّصة.
٢. التحقق من الالتزام بمتطلبات الإطار القانوني والرقابي لمواجهة غسل الأموال/مكافحة تمويل الإرهاب.
٣. تحديد التهديدات، ومكامن الضعف، والمخاطر الناشئة ذات الصلة بالقطاع المالي لدولة الإمارات.

**المحاكم الاتحادية لجرائم غسل الأموال:**

أصدرت وزارة العدل بدولة الإمارات قرارات وزارية بإنشاء محاكم متخصصة لنظر جرائم غسل الأموال بالقضاء الاتحادي بمحاكم الشارقة وعجمان وأم القيوين والفجيرة، حيث أُنشئت بكل دار قضاء دوائر جزئية وكلية ودوائر استئناف لنظر هذه الجرائم (وزراة الخارجية والتعاون الدولي، ٢٠٢١).

**المحاكم المحلية لجرائم غسل الأموال**

قرارًا بإنشاء محكمة متخصصة للنظر في جرائم غسل الأموال والتهرب الضريبي، وذلك في إطار تنفيذ الأولوية الاستراتيجية لدائرة القضاء المتمثلة بتعزيز فاعلية وكفاءة التقاضي وضمان منظومة العدالة الجنائية، وصولاً إلى هدف قضاء عادل وناجز (وزراة الخارجية والتعاون الدولي، ٢٠٢١).

**منصة مكافحة غسل الأموال وتمويل الإرهاب**

أطلقت وحدة المعلومات المالية في المصرف المركزي بالتعاون مع مكتب الأمم المتحدة المعني بالمخدرات والجريمة منصة رقمية (goAML) لجمع وتحليل المعلومات المالية بما يتوافق مع متطلبات مكافحة غسل الأموال، وأصبح التسجيل في برنامج (goAML) إلزاميًّا لجميع المؤسسات والشركات المالية مثل: البنوك ومكاتب الصرافة وشركات التمويل، وفقا للقانون. وسوف يسهم البرنامج الجديد في منع جرائم غسل الأموال وتمويل الإرهاب والأنشطة المالية الأخرى غير المشروعة، وسيكون البرنامج جزءًا من وحدة المعلومات المالية؛ حيث سيعزز من قدراتها بالإضافة إلى ضمان الحفاظ على فعالية النظام المالي الإماراتي في مواجهة غسل الأموال وتمويل الإرهاب.

يعزز إنشاء محكمة جرائم غسل الأموال والتهرب الضريبي جهود دولة الإمارات الفاعلة لمواجهة تلك الجرائم، وضمان ملاحقة مرتكبيها وتقديمهم للعدالة، عبر اتخاذ العديد من الخطوات والإجراءات بالتنسيق والتكامل مع مختلف الجهات المعنية (وزراة الخارجية والتعاون الدولي، ٢٠٢١).

**اللجنة الوطنية لمواجهة غسل الأموال ومكافحة تمويل الإرهاب والتنظيمات غير المشروعة**

تشرف اللجنة الوطنية لمواجهة غسل الأموال ومكافحة تمويل الإرهاب والتنظيمات غير المشروعة على عملية التقييم الوطني للمخاطر، كما تعمل على مواجهة مخاطر غسل الأموال وتمويل الإرهاب تماشيًا مع التزاماتها بموجب معايير مجموعة العمل المالي (فاتف، د.ت).

تتضمن مهام واختصاصات اللجنة ما يلي (وزراة الخارجية والتعاون الدولي، ٢٠٢١):

١. وضع استراتيجية وطنية لمكافحة الجريمة وتطويرها، واقتراح الأنظمة والإجراءات والسياسات ذات الصلة بالتنسيق مع الجهات المعنية، ومتابعة تنفيذها.
٢. تحديد مخاطر جريمة غسل الأموال وتقييمها.
٣. التنسيق مع الجهات المعنية والرجوع إلى مصادر المعلومات في الجهات الدولية ذات الصلة؛ لتحديد الدول عالية المخاطر في مجال غسل الأموال وتمويل الإرهاب، وتوجيه الجهات الرقابية بالتحقق من التزام المنشآت المالية والأعمال والمهن غير المالية المحددة والجمعيات غير الهادفة للربح الخاضعة لإشرافها بتطبيق التدابير الواجب اتباعها.
٤. تسهيل تبادل المعلومات، والتنسيق بين الجهات الممثلة فيها.
٥. تقييم فاعلية نظام مكافحة غسل الأموال وتمويل الإرهاب وتمويل التنظيمات غير المشروعة، من خلال جمع الاحصائيات وغيرها من المعلومات ذات الصلة من الجهات المعنية وتحليلها.
٦. تمثيل الدولة في المحافل الدولية المتعلقة بمواجهة غسل الأموال ومكافحة تمويل الإرهاب.
٧. اقتراح اللائحة التنظيمية الخاصة بعمل اللجنة وعرضها على الوزير لاعتمادها.

**(فوري تيك) منصة ذكية للكشف عن الجرائم المالية**

"فوري تيك" هو نظام ذكي يعمل على جمع القضايا المتصلة بغسل الأموال وتمويل الإرهاب من مختلف الجهات الاتحادية والمحلية، وتيسير التواصل فيما بينها؛ بهدف تسريع اتخاذ الإجراءات والقرارات في غضون ساعات.

يساعد نظام "فوري تيك" على تطبيق إجراءات صارمة من شأنها الاستجابة السريعة للحد من الجرائم المالية، وغسل الأموال، والقضاء على مصادر تمويل الإرهاب.

طُوِّرت منصة "فوري تيك" من قِبَل الهيئة الاتحادية للرقابة النووية (FANR) بإشراف اللجنة الفنية الفرعية التي تتضمّن أعضاء من اللجنة الوطنية لمواجهة غسل الأموال ومكافحة تمويل الإرهاب وتمويل التنظيمات غير المشروعة (البوابة الرسمية لحكومة الإمارات العربية المتحدة ، د.ت.)

مما سبق يتبين لنا أن دولة الإمارات تقوم بجهود كبيرة في مجال مكافحة تمويل الإرهاب؛ حيث تعزز نظام مواجهة غسل الأموال وتمويل الإرهاب من خلال قوانينها والخطوات التي تتخذها، كما تواصل الدولة مع وحدات الاستخبارات المالية الأخرى والمنظمات الدولية مثل مجموعة العمل المالي لمنطقة الشرق الأوسط، لرصد شبكات تمويل الإرهاب وإيقافها، بالإضافة إلى جمع وتحليل المعلومات المالية (وزراة الخارجية والتعاون الدولي، ٢٠٢١).

**المبحث الثاني: مفهوم الذكاء الاصطناعي وأهم تطبيقاته وادواره في مكافحة الإرهاب الالكتروني**

شهد العالم تغيرات كثيرة في مختلف المجالات مع ظهور الثورة الصناعية، ودعت مجموعة العمل المالي (FATF) إلى استخدام التكنولوجيا لتعريف وكشف أنشطة غسل الأموال وتمويل الإرهاب؛ حيث تترك المعاملات المالية آثارًا إلكترونية يمكن معالجتها وتحليلها من أجل تكوين نظرة ثاقبة حول السلوكيات المالية لأولئك المنخرطين في نشاط غير مشروع، أو حتى لإثبات الارتباط الإجرامي عن طريق تقنية التعلم الآلي المتميز بها الذكاء الاصطناعي، في دعم برامج مكافحة غسل الأموال، حيث يمتلك التعلم الآلي قدرة على التعامل مع كميات كبيرة من البيانات، المنظمة وغير المنظمة، وقدرته على اكتشاف أنماط السلوك المالي التي يقوم بها أولئك المنخرطون في نشاط غير مشروع (جمعة، ٢٠٢٤). وسوف نناقش في هذا المبحث مطلبين حول هذا الموضوع:

**المطلب الأول: تعريف الذكاء الاصطناعي وماهيته**

تتركز فكرة الذكاء الاصطناعي (AI) بتقليد القدرات الذهنية البشرية، وهي جزء من عِلم الحاسوب المعني بتصميم الأنظمة الذكية التي تتضمن مجموعة من الخصائص المرتبطة بالذكاء والتي يمكن ربطها بالسلوكيات البشرية العميقة. (Badaro & Aguero, 2013) يُعرِّف غُريوال الذكاء الاصطناعي على أنه: "نظامٌ يعتمد على

المحاكاة الميكانيكية، ويُستخدم لجمع المعرفة والمعلومات المتعلِّقة بمختلف القطاعات في العالم، ومعالجتها ونشرها للاستفادة منها بصورة ذكية وعملية."

تُعرف جوانب علم الحاسوب التي تعتمد على محاكاة سلوك الأفراد، وفقاً لأوكانا فيرناندیز وفالينزو إيبورتو وغارو فيرناندیز، بأنها توفِّر مجموعة متنوعة من الأساليب والتقنيات والأدوات لإنشاء نماذج وحلول للمشكلات (Fernandez et al., 2019).

يندرج الذكاء الاصطناعي تحت نوعين، حيث يركز النوع الأول على مهام ضيقة ومحددة، مثل السيارات ذاتية القيادة، ويُعرف بالذكاء الاصطناعي الضعيف. أما النوع الآخَر فيُعرف بالذكاء الاصطناعي القوي أو الذكاء العام الاصطناعي، وهو القادر على أداء معظم المهام المعرفية التي يمكن أن يؤديها الإنسان، بالإضافة إلى تطبيقه على أكثر من مشكلة (Ma & Siau, 2018).

**المطلب الثاني: دور الذكاء الاصطناعي في مواجهة تمويل الارهاب**

يلعب الذكاء الاصطناعي دورًا مؤثرًا في تسيير وإدارة وتشكيل حياة البشر، سواء في النواحي المادية والعملياتية أو الجوانب المعنوية والسياقات الفكرية والمرجعيات العقائدية المحركة لتوجهات وسلوك البشر، ويتم ذلك من خلال الاستفادة من الذكاء الاصطناعي في برمجة وتخصيص رسائل وحملات توجيه مدروسة بدقة للتأثير على مدركات وقناعات الأفراد والمجموعات البشرية، كما يتم الاستفادة من البرمجيات (الخوارزميات) في رصد وفرز البيانات وتحليل المعلومات واستخلاص دلالاتها لتتبع السلوك البشري والاتجاهات المحتملة والتنبؤ بها وتوقع أحداث معينة أو التعرف على القائمين بها، وذلك وفقًا لنماذج رياضية يتم من خلالها معالجة البيانات باستخدام الحواسيب.

التنبؤ: يسهم الذكاء الاصطناعي في تحديد الأشخاص الذين يمكن أن يتأثروا بالأفكار المتطرفة، سواء كانوا أعضاء في جماعات فكرية متطرفة أو تنظيمات إرهابية، وبالتالي يتم تحديد الأفراد المحتملين الذين يمكن تصنيفهم كإرهابيين أو متطرفين.

التحصين: يتم تطوير استخدام الذكاء الاصطناعي في هذا المجال عن طريق إنشاء برامج موجهة توجه المستهدفين المحتملين إلى مصادر معلوماتية محددة؛ بهدف توجيه الأفكار وتقليل خطر الانزلاق إلى دوائر الإرهاب.

الملاحقة: تُسهم تطبيقات الذكاء الاصطناعي في تحديد الجماعة أو الطرف أو الشخص المتورط في الأعمال الإرهابية، سواءً كانت تنفيذيةً أو تخطيطيةً، من خلال تحليل المعطيات المرتبطة بالعمليات التحقيقية، مثل: نوع العملية والمكان ونوع السلاح والهدف، ومقارنتها بالتاريخ السابق للجماعات أو الأفراد المشتبَه بهم باستخدام معايير محددة للتصفية والترتيب، كما توجد نماذج رياضية محددة حققت نسب دقة عالية تجاوزت ٨٠٪ (سامح، ٢٠٢٢).

توفر تقنية الذكاء الاصطناعي فوائد عديدة في مختلف مجالات الحياة، وخاصة في مكافحة التطرف والإرهاب؛ حيث تلعب دورًا إيجابيًا مهمًّا، وتتمثل أهم هذه الفوائد في تقليل الوقت والجهد المبذولين في عمليات البحث والتتبع، خاصة مع تزايد حجم المعلومات المعالجة وتعقيدها وتشابكها. وتُعد برمجيات الذكاء الاصطناعي التي تستخدم في أجهزة التصوير والمراقبة، بالإضافة إلى قواعد البيانات المصورة للأفراد، من التطبيقات الهامة في هذا السياق؛ حيث أصبحت تقنية التعرف على الوجه باستخدام الذكاء الاصطناعي أداة أساسية في تحديد هوية المتورطين في أعمال العنف والحوادث الإرهابية (سامح، ٢٠٢٢).

على الرغم من سهولة ظاهرة الآلية الحالية، إلا أنها فعليًا تُعدُّ بالغة التعقيد وذات أهمية كبيرة؛ فيمكن ملاحظة هذا الأمر عندما ننظر إلى الجهود البشرية والمالية والوقت التي كان يتعين توظيفها سابقًا باستخدام أساليب وأدوات التعرف التقليدية والتتبع، حيث كان يستغرق ذلك وقتًا طويلًا يصل إلى عدة شهور، ولكن بفضل تقنيات الذكاء الاصطناعي، أصبح بإمكاننا القيام بنفس المهام في ثوانٍ قليلة (راشـد، ٢٠٢٢).

بفضل استخدام الذكاء الاصطناعي، يتم تضييق دوائر الاشتباه وتحديد المتورطين بدقة أكبر في مراحل البحث والتحري والملاحقة، وتسهيل عمليات الحصر والفرز للمعلومات والأشخاص وكل المعطيات ذات الصلة، مما يؤدي إلى تحسين الكفاءة والدقة في الجانب الأمني المباشر لمواجهة الإرهاب. وبالإضافة إلى ذلك، يخلق استخدام الذكاء الاصطناعي مناخًا من الثقة في أجهزة الأمن، ويوفر طمأنينة لدى الرأي العام تجاه المؤسسات والآليات المنخرطة في تلك المواجهة (راشـد، ٢٠١٩).

يشير "ماكيندريك" إلى وجود طريقتين لمنع الهجمات الإرهابية؛ الطريقة الأولى: هي الردع من خلال حماية البنية التحتية وتطبيق الضوابط الأمنية، والطريقة الثانية: هي التنبؤ؛ حيث يسهم التنبؤ في الحماية المادية للبنية التحتية، ويمكن استخدامه كوسيلة لتحسين تخصيص الموارد للمواقع التي من المحتمل أن تكون أهدافًا للإرهابيين.

تتضمن الاستراتيجية الثانية مكافحة الإرهاب من خلال الوقاية من الهجمات وتفكيك خلايا الإرهاب قبل تنفيذ مخططاتهم، ومنع تجنيد المتطرفين في المستقبل، وفرض قيود على حرية حركة الأفراد، كما يساعد التنبؤ الفعال في استخدام الإجراءات القسرية ضد المتطرفين العنيفين، في حين يتم استخدام الإجراءات التصالحية مع الأفراد المعرضين للتطرف (Kathleen, 2019).

تُعَدُّ وزارة الدفاع الأمريكية نموذجًا حيًّا لاستخدام التقنيات الذكية، بما في ذلك الذكاء الاصطناعي لمكافحة الجريمة المنظمة والإرهاب، وتُعَدُّ استراتيجيات الذكاء الاصطناعي (٢٠١٨)، والتحديث الرقمي (٢٠١٩)، والبيانات (٢٠٢٠)، التي أصدرتها الوزارة، أمثلة حية على هذا النوع من الاستخدام (الحقيل، ٢٠٢١) وفيما يلي بعض التطبيقات العملية:

١. أعلنت وكالة مشروع الأبحاث الدفاعية المتقدمة (DARPA) عن حملة "AI Next" التي تهدف إلى استثمار أكثر من ملياري دولار على مدى عدة سنوات في برامج جديدة وموجودة مع التركيز على المجالات الرئيسة التي تهم المنظمة.

٢. في عام ٢٠١٨، تم إطلاق مركز الذكاء الاصطناعي المشترك (JAIC) التابع لوزارة الدفاع، والذي يمثل المحور الرئيس لاستراتيجية الذكاء الاصطناعي للوزارة، وذلك لتنسيق ودمج الجهود والاستثمارات في هذا المجال.

٣. في العام نفسه، قامت قيادة العمليات الخاصة الأمريكية (SOCOM) بإجراء تغيير تنظيمي مشابه عن طريق إنشاء مكتب بيانات القيادة المصمم لمراقبة تحوُّل القوى العاملة، وكذلك توفير منصة للاتصالات الصناعية وإدارة البيانات والتطبيقات التي تركّز على البيانات في عمليات صنع القرار لتعزيز قدراتهم.

٤. لعبت JAIC وSOCOM والمركز الوطني الأمريكي لاستغلال وسائل الإعلام (NMEC) دورًا كبيرًا في استخدام "البيانات الضخمة" باستخدام التعلم الآلي والذكاء الاصطناعي، لمحاربة داعش وتنظيم القاعدة، ووكلاء الجماعات المتطرفة في العديد من البلدان (محمد، ٢٠٢٢)

٥. استخدمت وزارة الدفاع "خوارزميات مدربة خصيصًا" لحصر البيانات المختلفة والبحث عن الكيانات الإرهابية وتحديدها وتصنيفها، وتم التركيز على البيانات وعناصر العلم الضرورية لرسم خططها لمكافحة الجرائم ذات الصلة (محمد، ٢٠٢٢)

٦. يوجد سبب رئيس للحاجة إلى تطوير خطة عمل جديدة لإدارة البيانات، وهو تحديد الجريمة المنظمة والإرهاب وغيرها من الجرائم التي تهدد الأمن القومي، بالإضافة إلى تحسين العلاقات الدولية وتحقيق الأمن الداخلي والخارجي، وفيما يتعلق بفرنسا، تم استخدام أجهزة الاستخبارات الفرنسية بشكل عملي لتطبيق الخوارزميات المرتبطة بتقنيات الذكاء الاصطناعي وعلوم البيانات لمكافحة الإرهاب، وذلك من خلال معالجة سريعة للبيانات الوصفية التي يتم جمعها وتحليلها عبر "صناديق سوداء" المثبتة في النقاط الرئيسة للشبكة لدى مقدمي خدمات الإنترنت والاتصالات، وتعتبر هذه الخوارزميات تقنيات أكثر دقة من التحليل البشري لكميات هائلة من البيانات. (الحقيل، ٢٠٢١).

وهنا يتبادر إلى الذهن سؤال وهو: كيف يمكن استخدام الذكاء الاصطناعي في مكافحة الإرهاب؟ قدرات الذكاء الاصطناعي ليست قاصرة على استخدام الجماعات الإرهابية لها فقط، ولكن من الممكن أن تقوم الدول والحكومات وأجهزة المخابرات باستخدام الذكاء الاصطناعي في التنبّؤ والتعرف على الجماعات الإرهابية والقدرة على منعهم من القيام بعملياتهم الإرهابية من الأساس، وفي هذا السياق سنستعرض أربع طرائق لكيفية استخدام الذكاء الاصطناعي في مكافحة العمليات الإرهابية:

**١. المساعدة في تقويض الأفكار المتطرفة**

من المعروف أن الجماعات الإرهابية تستخدم الذكاء الاصطناعي لعمل فيديوهات وصور تروّج لأفكارها الإرهابية لجذب تعاطف المستخدمين العاديين؛ لذا من الممكن أن تقوم الدول باستخدام الذكاء الاصطناعي في التعرف على ذلك المحتوى الذي يحمل أفكارًا إرهابية وتقوم بحجبه، بل تقوم بتصدير محتوى مضاد يحمل حقائق مخالفة للأفكار الإرهابية المرَوَّجة.

فعلى سبيل المثال، هناك تجربة في عام ٢٠١٦ قامت بها جوجل باستخدام الذكاء الاصطناعي (Jigsaw) والتي من خلالها قامت جوجل بتحديد مؤشرات معينة مرتبطة بتنظيم داعش، إذا ظهرت في محرك البحث لدى المستخدم تقوم بتوجيهه تلقائيًّا إلى فيديوهات ومواقع أخرى تعرِض له محتوى مضادًّا لما بُحث عنه وله علاقة بتنظيم داعش (UNICRI, 2021).

**٢. المساعدة في تحديد توقيت وموقع الهجمات الإرهابية المحتملة**

تم عمل عدد من النماذج التي تعتمد على استخدام الذكاء الاصطناعي لتحديد مكان وتوقيت الهجمات الإرهابية من خلال تتبع استخدام أفراد الجماعات الإرهابية للإنترنت، والمعاملات البنكية، وحجوزات الطيران الخاصة بهم، وما إلى ذلك، وفي عام ٢٠١٥ استُخدِم أحد تلك النماذج التنبؤية، والتي نجحت بالفعل في التنبّؤ بهجمة إرهابية انتحارية بنسبة دقّة وصلت إلى ٧٢ % (UNICRI, 2021).

**٣. المساعدة في تحديد احتمالية أن يكون الشخص إرهابيًّا**

من الممكن للحكومات أن تَستخدم الذكاء الاصطناعي في التعرف على احتمالية أن يكون المستخدم إرهابيًّا، أو أنه سيكون إرهابيًّا في المستقبل، ومن الأمثلة على ذلك ما قامت به وكالة الأمن القومي الأمريكية في عام ٢٠٠٧ من استخدام خاصية تشبه الذكاء الاصطناعي بشكله الحالي المتعارف عليه، وخلصت إلى أن هناك ١٥ ألف مواطن باكستاني من أصل ٢٠٠ مليون باكستاني –آنذاك– من الممكن أن يكونوا إرهابيين في ذلك الوقت، أو لديهم فكْر متطرف، على الرغم من عدم إثبات نسبة دقّة ذلك النموذج فإنه وارد الاستخدام، ومن الممكن أن يتم تطويره الآن مع تقدم التكنولوجيا عامةً، والذكاء الاصطناعي خاصة.

أما في المساعدة في التعرف على وجه الإرهابيّين، فقد يكون الذكاء الاصطناعي عاملًا أساسيًّا تعتمد عليه الحكومات في التعرف على وجوه الأشخاص المنتمين إلى جماعات إرهابية، والذين تودّ الحكومات أن تقوم بتحديد أماكنهم، فعلى سبيل المثال قامت الشرطة الفيدرالية الألمانية في عامَي ٢٠١٧ و٢٠١٨ بتركيب كاميرات تتضمن خاصية التعرف على الوجوه –والتي تعتمد على الذكاء الاصطناعي– في محطة قطار ألمانية تُعدُّ من أكثر المحطات ازدحامًا، بهدف التعرف على عناصر الجماعات الإرهابية المطلوبين لدى الحكومة الألماني (UNICRI, 2021).

**٤. المساعدة في تعقب تمويل الإرهاب**

هناك تطبيقات وبرامج مثل OSIN (Open Source Intelligence) والتي هي تقنية تتكون من جمع وتحليل المعلومات من مصادر خارجية، مثل: الوسائط والشبكات الاجتماعية والمنتديات عبر الإنترنت والمدونات لتعقُّب تمويل الإرهاب، حيث يمكِّن OSINT المحللين الماليين المتخصصين في الإرهاب من استخدام الأدوات الآلية لجمع وتحليل البيانات المستمدة من مصادر متعددة، ما يسهل الكشف عن الأنشطة المشتبه بها بسرعة ودقّة (Hadar, 2023).

فمن الممكن أن يُقلّص الذكاء الصناعي –إلى حدّ بعيد– من احتمالات الخطأ في مراحل البحث والتحري، وتحديد المتورطين، وكذلك في مراحل الملاحقة، والسعي إلى إنفاذ القانون (راشـد، ٢٠٢١).

وأيضا تحسين عملية صنع القرار في مكافحة التطرف والإرهاب، وكذلك في تحليل البيانات الضخمة لأغراض مكافحة الإرهاب (Almukhtan, 2023)؛ فمن الممكن أن يُقلّص الذكاء الصناعي –إلى حدّ بعيد– من احتمالات الخطأ في مراحل البحث والتحري، وتحديد المتورطين، وكذلك في مراحل الملاحقة، والسعي إلى إنفاذ القانون (راشـد، ٢٠٢١).

**الخاتمة**

يُعدُّ الإرهاب الإلكتروني من أخطر أشكال الإرهاب في العالم؛ ويأتي ذلك نظرًا لدور الفضاء الإلكتروني الاستراتيجي في المجتمع الدولي في المجالات الاقتصادية والسياسية والثقافية والأمنية والاجتماعية، كما أن خطر الأعمال الإرهابية الإلكترونية يكمن في استخدام تقنيات متقدمة مثل: أجهزة التنصت على شبكات الاتصالات، وبرامج التشفير والاختراق والتلاعب بأنظمة الأمان. ومع احتواء الشبكات الآلية على عشرات الآلاف أو ملايين الأجهزة المرتبطة بالإنترنت، يمكن استخدامها للقيام بأنواع مختلفة من الهجمات الجرمية مثل: الإرهاب والتخريب والابتزاز والتهديد. لذلك يُعدُّ التركيز على تطوير الذكاء الاصطناعي أمرًا ضروريًا لضمان استمرار الرفاهية البشرية ومن خلال دراستنا توصلنا إلى النتائج و التوصيات التالية:

**أولاً: أهم النتائج**

توصَّل الباحث إلى مجموعة من النتائج:

١. حظي مفهوم الذكاء باهتمام العلماء والباحثين منذ القِدم؛ حيث اهتموا بدراسته من جوانب عِدة، وقدموا عددًا كبيرًا من النظريات التي تفسِّر طبيعته، الأمر الذي أدى إلى تعدُّد تعريفاته.

٢. يشكِّل المجال العسكري والسياسي أحد أهم مجالات الذكاء الاصطناعي؛ حيث يرتبط الذكاء الاصطناعي –في غالبية الدول الصناعية الكبرى وخاصة الولايات المتحدة الامريكية وبريطانيا– بالمجال العسكري؛ وذلك لأرضية الدعم الذي يعتمد عليها هذا المجال.

٣. إن المشرع الإماراتي لم يكتفِ بتعريف تمويل الإرهاب، ولكنه أورد تعريفًا لتمويل التنظيمات الإرهابية، ومن ثَمَّ فالاتجاه الغالب يميل نحو تعريف تمويل الإرهاب بوصفه نموذجًا إجراميًّا مستقلًا، على الرغم من الربط بينه وبين غسل الأموال.

٤. كما أظهرت الدراسة التطور في صور وأساليب تمويل الإرهاب، والذي عكسته الاتفاقية العربية لمكافحة غسل الأموال وتمويل الإرهاب، والتي جاءت بعد الاتفاقية الدولية لقمع تمويل الإرهاب بعشر سنوات، والتي كانت تقصر التمويل على صورتَي جمع وتقديم الأموال، وقد توسع المشرع الإماراتي في صور التمويل لتشمل حيازة أو حفظ أو إدارة أو استثمار الأموال المعدة لتمويل الإرهاب.

٥. المشروع الإماراتي عمل على مواجهة تمويل الإرهاب بكافة الأشكال والطرق وذلك من خلال سن القوانين وتعديلها.

٦. يلقى الذكاء الاصطناعي وتطبيقاته في المجالات المتعلقة بمكافحة تمويل الإرهاب الإلكتروني والإرهاب بشكل عام دعمًا كبيرًا؛ حيث يتم تطوير تقنيات باستخدام الذكاء الاصطناعي تعمل على مواجهة الإرهاب.

**ثانياً: أهم التوصيات**

ومن خلال هذه الدراسة يمكن التوصية بما يلي:

١. ضرورة تحقيق التناسق بين التشريعات الجنائية الإماراتية الخاصة بمكافحة غسل الأموال وتمويل الإرهاب وتلك المتعلقة بمكافحة الإرهاب بصدد جريمة تمويل الإرهاب، وذلك من حيث المساواة بين "الأموال" "والمتحصلات" كمصادر لتمويل الإرهاب؛ وذلك لتوحيد صور السلوك الإجرامي التي ترد على كل منهما.

٢. نعتقد أنه من باب التناسق التشريعي أن تكون المادة ٣ الخاصة بتمويل الإرهاب والواردة في المرسوم بقانون اتحادي رقم (٢٠) لسنة ٢٠١٨، ضمن مواد القانون رقم ٧ لسنة ٢٠١٤ بشأن مكافحة الإرهاب، وأن يتم تعديل مسمى القانون الأخير ليصبح "قانون مكافحة الإرهاب وتمويله"؛ منعًا لإمكانية حدوث ازدواجية في التجريم والعقاب، أو حدوث تضارب بين النصوص العقابية، أو تفرقة غير مبررة بين مظاهر السلوك الإجرامي في جريمة واحدة "تمويل الإرهاب"، وحتى لا تكون هناك ثغرات يمكن أن ينفذ من خلالها مموّلو الإرهاب والجماعات الإرهابية.

٣. ضرورة التعاون بين الإمارات والدول الأخرى في الجانب الإقليمي لمكافحة الإرهاب الإلكتروني؛ إذ يمكن لأغلب الدول العربية التي تدعو إلى التسامح والمحبة أن تتخلص من أعمال الإرهاب الإلكتروني التي تهدد أمن واستقرار المنطقة. من الممكن تطوير التعاون على المستوى بحيث تكون هناك مواثيق

ومعاهدات دولية تسهم في مكافحة العمليات الإرهابية الإلكترونية، كما هو الحال مع المواجهة الأكثر عمومية مع الإرهاب الدولي.

٤. ضرورة العمل على تطوير الذكاء الاصطناعي من أجل مواجهة جميع أشكال الإرهاب، وذلك من خلال إنشاء منظومة قانونية وأخلاقية تحكم عملية الاستعانة بتقنيات الذكاء الاصطناعي.

## المراجع

أسامة جابر محمد دودح. (٢٠١٦). جريمة الإرهاب الإلكتروني في التشريع الأردني. رسالة ماجيستير منشورة، كلية الحقوق–جامعة جرش.

باسم راشد. (٢٠١٩). فرص ومخاطر استخدامات الذكاء الإصطناعي في مكافحة الإرهاب. المستقبل للأبحاث والدراسات الإستراتيجية.

البوابة الرسمية لحكومة الإمارات العربية المتحدة . (د.ت). البوابة الرسمية لحكومة الإمارات العربية المتحدة | مكافحة غسل الأموال. https://u.ae/ar-ae/information-and-services/business/regulations/combatting-money-laundering

البوابة الرسمية لحكومة الإمارات العربية المتحدة. (٢٠٢٣). https://u.ae/ar-ae/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security

الجخة، عادل. (٢٠٠٩). أثر الإرهاب الإلكتروني على مبدأ استخدام القوة في العلاقات الدولية (٢٠٠١–٢٠٠٧). رسالة ماجستير في العلوم السياسية. القاهرة: جامعة القاهرة: كلية الاقتصاد والعلوم السياسية.

جريدة الاتحاد. (٣ مارس ٢٠٢٢). الصفحة الاقتصادية. أبو ظبي.

جودت، هوشيار. (٢٠١٤). العلاقة الملتبسة بين الإعلام والإرهاب. https://middle-east-online.com/id=188043

سامح راشد. (٢٠٢١). الذكاء الاصطناعي في مواجهة الإرهاب. فرص وتحديات. مركز المعلومات واتخاذ القرار.

سامح راشد. (٢٠٢٢). الذكاء الاصطناعي في مواجهة الإرهاب–فرص وتحديات. مجلة درع الوطن.

شريف عبدالرحمن، رمضان. (٢٠١٦). الإرهاب الدولي – أسبابه وطرق مكافحته في القانون الدولي والفقه الإسلامي: دراسة مقارنة. كلية الشريعة والأنظمة، جامعة الطائف، المملكة العربية السعودية، ٣١ (٣)، ١١٠٧.

طارق جمعة. (٢٠٢٤). الذكاء الاصطناعى و تمويل الإرهاب وغسل الأموال. مركز رع للدراسات الاستراتيجية.

عادل عبد الصادق. (٢٠٠٧). "هل يمثل الإرهاب شكلًا جديدًا من أشكال الصراع الدولي" ملف الأهرام الاستراتيجي. مركز الدراسات السياسية والاستراتيجية، ١٥٦، ١٥.

عادل عبد الصادق. (٢٠٠٩). الإرهاب الإلكتروني: القوة في العلاقات الدولية نمط جديد وتحديات مختلفة. مركز الدراسات السياسية والاستراتيجية، ١٠٩.

عبد الوهاب الكيالي. (١٩٩٤). الموسوعة السياسية. بيروت: المؤسسة العربية للدراسات والنشر.

علاء الدين راشد. (٢٠٠٦). المشكلة في تعريف الإرهاب. القاهرة، مصر: دار النهضة.

غسان أبو مويس. (٢٠٢٠). أمانة مجلس محافظي المصارف المركزية ومؤسسات النقد العربية–دراسة حول جهود الدول العربية على صعيد مكافحة غسل الأموال وتمويل الإرهاب. https://www.amf.org.ae/sites/default/files/publications/2022-01/efforts-of-arab-countries-in-terms-of-combating-money-laundering-and-terrorist-financing.pdf

فاتف. (د.ت). اللجنة الوطنية لمواجهة غسل الأموال ومكافحة تمويل الإرهاب والتنظيمات غير المشروعة. https://www.fatf-gafi.org/en/home.html

المادة (٣٠) القانون الاتحادي رقم( ٧) لعام ٢٠١٤ – الإمارات.

المادة رقم (٣) (القانون الاتحادي رقم (٢٠) لعام ٢٠١٨– الإمارات.

المادتين (٢٩–٣٠) (القانون الاتحادي رقم (٧) لعام ٢٠١٤– الإمارات.

مكتب الأمم المتحدة المعني بالمخدرات والجريمة. (٢٠١٣). استخدام الإنترنت في أغراض إرهابية. الأمم المتحدة–نيويورك، صفحة ٦.

ملا خاطر، و مايا حسن. (٢٠١٥). الإطار القانوني لجريمة الإرهاب الإلكتروني. مجلة جامعة الناصر، ٥(١)، ١٣٣–١٣٤.

نجلاء عبد الرحمن الحقيل. (٢٠٢١). فعالية الذكاء الاصطناعي لمكافحة الجريمة والإرهاب. https://www.alarabiya.net/aswaq/opinions/2021/11/17/%D9%81%D8%B9%D8%A7%D9%84%D9%8A%D8%A9-%D8%A7%D9%84%D8%B0%D9%83%D8%A7%D8%A1-%D8%A7%D9%84%D8%A7%D8%B5%D8%B7%D9%86%D8%A7%D8%B9%D9%8A-%D9%84%D9%85%D9%83%D8%A7%D9%81%D8%AD%D8%A9-%D8%A7%D9%84%D8%AC%D8%B1%D9%8A%.

وجيه محمد. (٢٠٢٢). كيف يستخدم الذكاء الاصطناعي في مواجهة الجريمة المنظمة والإرهاب؟ https://m.akhbarelyom.com/news/newdetails/3839711/1/%D9%83%D9%8A%D9%81-%D9%8A%D8%B3%D8%AA%D8%AE%D8%AF%D9%85-%D8%A7%D9%84%D8%B0%D9%83%D8%A7%D8%A1-%D8%A7%D9%84%D8%A7%D8%B5%D8%B7%D9%86%D8%A7%D8%B9%D9%8A-%D9%81%D9%8A-%D9%85%D9%88%D8%A7%D8%AC%D9%87%D8%A9-%D8%A.

وزراة الخارجية والتعاون الدولي. (٢٠٢١). وزراة الخارجية والتعاون الدولي. https://www.mofa.gov.ae/ar-AE/MediaHub/News/2023/12/31/31-12-2023-UAE-Abu-Dhabi

وسام حسام الدين، الأحمد. (د.ت). مكافحة الجريمة المنظمة عبر الوطنية في ضوء أحكام الشريعة الإسلامية والأنظمة السعودي، ١.

وكالة أنباء الإمارات. (٣ مارس ٢٠٢٢). https://www.wam.ae/ar/home/main

**REFERENCES**

Almukhtan, Obaid. (2023). *Exploitation Des Outils De L ̂intelligence Artificielle Dans La Lutte Contre Le Terrorisme*. Islamic Military Counter Terrorism Coalition.

Badaro, I., & Aguero. (2013). Expert Systems: Fundamentals, Methodologies and Applications. *Cienciay Technology, 13*, 349-364.

Denning, D. E. (2000). *Cyber terrorism*. Global Dialogue, 3(1).

Dogrul, M., Aslan, A., & Celik, E. (2011). *Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism*. C. Czosseck, E. Tyugu, T. Wingfield (Eds.) Tallinn, Estonia. 3rd International Conference on Cyber Conflict. CCD COE Publications

Fernandez, O., Fernandez, G., & Aburto, V. (2019). Artificial Intelligence and its Implications in Higher Education. *Propositions y Representations. 7*(2), 536-568.

Hadar, J. (2023). Et si l'IA entravait le financement du terrorisme en Afrique. Jeune Afrique, (34). https://www.jeuneafrique.com/1489042/politique/et-si-lia-entravait-le-financement-du-terrorisme-en-afrique/

Kathleen, M. (2019). *Artificial Intelligence Prediction and Counterterrorism.* Chatham House. The Royal Institute of International Affairs.

Ma, Y., & Siau, K. (2018). *Artificial Intelligence Impacts on Higher Education*. Proceedings of the Thirteenth Midwest Association for Information Systems Conference. Saint Louis, Missouri.

UNICRI. (2021). Countering Terrorism Online with Artificial Intelligence – an Overview for Law Enforcement and Counter-Terrorism Agencies in South Asia and South-East Asia. https://unicri.it/Publications/Countering-Terrorism-Online-with-Artificial-Intelligence-%20SouthAsia-South-EastAsia

Weimann, G. (2006). Terror on the Internet: The New Arena, the New Challenges Washington. D.C.: United States Institute of Peace Press, 13(11), 37.

**إنكار**

الآراء الواردة في هذه المقالة هي آراء المؤلف. "فردانا: المجلة العالمية في البحوث الأكاديمية" لن تكون مسؤولة عن أي خسارة أو ضرر أو مسؤولية أخرى بسبب استخدام مضمون هذه المقالة.