گوڤارا ئەکادیمی یا زانکویا نەوروز (المجلة الأكاديمية لجامعة نوروز)، پ.١ ژ.١، ٢٠٢٣

https://doi.org/10.25007/ajnu.v1n1a1960

دور الذكاء الاصطناعي في مواجهة جرائم الإرهاب الإلكتروني

(دراسة مقارنة)

د. رانا مصباح عبد المحسن عبد الرازق، أستاذ القانون الجنائي المساعد بدبلوم القانون، مديرة برنامج دبلوم القانون بالكلية التطبيقية جامعة الأميرة نورة بنت عبد الرحمن بالرياض، مملكة العربية السعودية

ملخص

هدفت هذه الدراسة إلى بيان دور الذكاء الاصطناعي في التصدي لجرائم الإرهاب الإلكتروني، ولذلك تخضع بيانات الإرهابيين أو المتهمين الخطرين لتطبيقات الذكاء الاصطناعي التي تضطلع بكشف الجرائم قبل ارتكابها، فقد طورت الجماعات والتنظيمات الإرهابية قدراتها التكنولوجية بما سمح لها باستخدام بيانات ضخمة وتحليلها عبر الإنترنت بغرض تسهيل عملياتها الإرهابية، والتجنيد الإلكتروني للشباب من خلال الشبكة العنكبوتية.

واعتمدت الدراسة على استخدام المنهج الوصفي التحليلي بالإضافة إلى الاستعانة بالمنهج المقارن، واشتملت هذه الدراسة على ثلاثة مباحث: تناولت بيان ماهية الذكاء الاصطناعي، والتعرف على دور أنظمة الذكاء الاصطناعي في مواجهة جرائم الإرهاب الإلكتروني، وأيضاً التعرف على التنظيم القانوني لجرائم الإرهاب الإلكتروني، وأخيراً التعرف على موقف التشريعات والاتفاقيات العربية من مواجهة جرائم الإرهاب الإلكتروني. وتوصلت الدراسة للعديد من التوصيات ومنها، ضرورة إنشاء محكمة دولية للأمن الإلكتروني للتعاون القضائي الجنائي الدولي، والإبلاغ عن القضايا الإرهاب الإلكتروني.

الكلمات المفتاحية: الذكاء الاصطناعي، الخوارزميات، الإرهاب الإلكتروني، تقنيات المعلومات، تكنولوجيا المعلومات، الشبكة المعلوماتية.

1. المقدمة

أصبحت تقنيات الذكاء الاصطناعي من أهم آثار تكنولوجيا المعلومات الحديثة، حيث أصبح الذكاء الاصطناعي يدخل في أغلب مجالات الحياة، ومنها مجال التحقيق والتحري عن الجرائم، لما له من أهمية كبيرة في منع وقوع الجرائم، والعمل على كشفها والتنبؤ بالمخاطر المترتبة عليها، لذلك لا يُمكن لأنظمة الذكاء الاصطناعي التنبؤ بجرائم الإرهاب الإلكتروني بدون خوارزميات مُتخصّصة ومُعدّة لذلك.

1.1 مشكلة الدراسة

تمكن مشكلة الدراسة في ظهور أنماط جديدة من الجرائم، كالجرائم التي ترتكب عبر وسائل الانترنت، وبالأخص جرائم الإرهاب الإلكتروني، والتي تعتبر من أهم التهديدات الأمنية الخطيرة التي تهدد المجتمع الدولي، والسبب في ذلك اتباع المنظمات الإرهابية المتطرفة طرق ووسائل التقنية الحديثة للتواصل بين قياداتها وأعضائها، وتجنيد الأشخاص، والتخطيط للعمليات الإرهابية، والتجسس الإلكتروني. لذلك كان لابد من التصدي للإرهاب الإلكتروني من خلال استخدام المحققين لأنظمة الذكاء الاصطناعي، نظراً لما له من قدرة على اكتشاف الجرائم ومعرفة مرتكبيها، ووضع القوانين والتشريعات والاتفاقيات التي تساهم في الحد من هذه الجرائم.

وبناءً على ذلك تتمثل مشكلة الدراسة بصفة أساسية في التساؤل الرئيس الآتي:

ما دور الذكاء الاصطناعي والأنظمة القانونية في التصدي لجرائم الإرهاب الإلكتروني؟

وينبثق من هذا السؤال الرئيس الأسئلة الفرعية الآتية:

- ما المقصود بماهية الذكاء الاصطناعي؟
- ما دور أنظمة الذكاء الاصطناعي في مواجهة جرائم الإرهاب الإلكتروني؟
- ما أركان جرائم الإرهاب الإلكتروني؟
- ما صور جرائم الإرهاب الإلكتروني؟
- ما وسائل الإرهاب الإلكتروني؟
- ما موقف التشريعات العربية من مواجهة جرائم الإرهاب الإلكتروني؟
- ما موقف الاتفاقيات العربية من مواجهة جرائم الإرهاب الإلكتروني؟

2.1 أهداف الدراسة

بناء على مشكلة الدراسة وتساؤلاتها تهدف الدراسة إلى الآتي:

- التعرف على ماهية الذكاء الاصطناعي.
- التعرف على أنظمة الذكاء الاصطناعي في مواجهة جرائم الإرهاب الإلكتروني.
- التعرف على أركان جرائم الإرهاب الإلكتروني.

- التعرف على صور جرائم الإرهاب الإلكتروني.
- التعرف على وسائل الإرهاب الإلكتروني.
- التعرف على موقف التشريعات العربية من مواجهة جرائم الإرهاب الإلكتروني.
- التعرف على موقف الاتفاقيات العربية من مواجهة جرائم الإرهاب الإلكتروني.

3.1 أهمية الدراسة

تبرز أهمية هذه الدراسة من خلال أهمية الموضوع الذي تتناوله، حيث إنه مع تزايد التطور العلمي لتكنولوجيا المعلومات أدى ذلك إلى ظهور وسائل تقنية جديدة كالذكاء الاصطناعي الذي يمكن المحققين في جرائم الإرهاب من الوصول إلى جمع الأدلة بطرق احترافية. وتتبدّى فاعلية التنبؤ الخوارزمي بجرائم الإرهاب بُغية منعها قبل حدوثها، والقدرة على الحدّ من الهدر في الوقت والمجهود في البحث والتنقيب، فتطبيقات الذكاء الاصطناعي تحتوي على خوارزميات لمطابقة الوجوه، والأصوات، والتعرّف بدقة على التصرفات الإرهابية التي تُنبئ عن احتمال وقوع جريمة إرهابية ما. ولذلك كان لا بد على الدول إيجاد تشريعات قانونية لمواجهة ظاهرة الإرهاب الإلكتروني.

4.1 منهج الدراسة

اعتمدت الدراسة على المنهج الوصفي التحليلي الذي يقوم على أساس تحديد ماهية الذكاء الاصطناعي، والتعرف على دور أنظمة الذكاء الاصطناعي في مواجهة جرائم الإرهاب الإلكتروني، وأيضاً التعرف على التنظيم القانوني لجرائم الإرهاب الإلكتروني، وأخيراً التعرف على موقف التشريعات والاتفاقيات العربية من مواجهة جرائم الإرهاب الإلكتروني، بالإضافة إلى الاستعانة بالمنهج المقارن من خلال تحليل النصوص القانونية المقارنة.

5.1 حدود الدراسة

1.5.1 الحدود الموضوعية

اقتصرت الدراسة على التطرق إلى بيان تشريعات المملكة العربية السعودية فيما يتعلق بمكافحة جرائم الإرهاب الإلكتروني، وكذلك التعرف على أنظمة الذكاء الاصطناعي ودورها في مواجهة جرائم الإرهاب الإلكتروني، والتعرف على صور جرائم الإرهاب الإلكتروني وأركانها.

2.5.1 الحدود الزمانية

تم إجراء هذه الدراسة في الفصل الدراسي الثاني للعام الجامعي 1444هـ- 2023م.

3.5.1 الحدود المكانية

اقتصرت الدراسة على المملكة العربية السعودية، ومصر، والإمارات، وإقليم كوردستان – العراق.

6.1 مصطلحات الدراسة

1.6.1 الذكاء الاصطناعي

هو فرع من فروع الحاسوب يهتم بدراسة أنظمة حاسوبية وصناعتها يمكنها إنجاز أعمال تتطلب ذكاءً بشريًا، حيث تمتاز هذه الأنظمة بأنها تتعلم مفاهيم ومهام جديدة ويمكنها أن تفكر وتستنتج استنتاجات مفيدة حول العالم الذي نعيش فيه.

2.6.1 الخوارزميات

هي من الخطوط الرياضية والمنطقية والمتسلسلة اللازمة لحل مشكله ما.

3.6.1 النظام المعلوماتي

مجموعة برامج وأدوات معدة لمعالجة البيانات وإدارتها، وتشمل الحاسبات الآلية.

4.6.1 الشبكة المعلوماتية

ارتباط بين أكثر من حاسب آلي أو نظام معلوماتي للحصول على البيانات وتبادلها، مثل الشبكات الخاصة والعامة والشبكة العالمية (الإنترنت).

5.6.1 وسيلة تقنية المعلومات

أي أداة إلكترونية مغناطيسية، بصرية، كهروكيميائية، أو أي أداة أخرى تستخدم لمعالجة البيانات الإلكترونية وأداء العمليات المنطقية والحسابية، أو الوظائف التخزينية، ويشمل أي وسيلة موصلة أو مرتبطة بشكل مباشر، تتيح لهذه الوسيلة تخزين المعلومات الإلكترونية أو إيصالها للآخرين.

6.6.1 الإرهاب الإلكتروني

العدوان، أو التخويف، أو التهديد المادي، أو المعنوي، الصادر من الدول أو الجماعات أو الأفراد على الإنسان، باستخدام الموارد المعلوماتية أو الوسائل الإلكترونية.

7.6.1 الإرهابي

أي شخص ذي صفة طبيعية -سواء أكان في المملكة أو خارجها- يرتكب، أو يشرع أو يشترك أو يخطط أو يساهم في ارتكابها، بأي وسيلة مباشرة أو غير مباشرة.

8.6.1 الجماعة الإرهابية

كل سلوك يقوم به الجاني تنفيذاً لمشروع إجرامي فردي أو جماعي بشكل مباشر أو غير مباشر، يقصد به الإخلال بالنظام العام، أو زعزعة أمن المجتمع واستقرار الدولة أو تعريض وحدتها الوطنية للخطر، أو تعطيل النظام الأساسي للحكم أو بعض أحكامه، أو إلحاق الضرر بأحد مرافق الدولة أو مواردها الطبيعية أو الاقتصادية، أو محاولة إرغام إحدى سلطاتها على القيام بعمل ما أو الامتناع عنه، أو إيذاء أي شخص أو التسبب في موته، عندما يكون الغرض -بطبيعته أو سياقه- هو ترويع الناس أو إرغام حكومة أو منظمة دولية على القيام بأي عمل أو الامتناع عن القيام به، أو التهديد بتنفيذ أعمال تؤدي إلى المقاصد والأغراض المذكورة أو التحريض عليها.

9.6.1 جريمة تمويل الإرهاب

توفير أموال لارتكاب جريمة إرهابية أو لمصلحة كيان إرهابي أو إرهابي، بما في ذلك تمويل سفر إرهابي وتدريبه.

7.1 الدراسات السابقة

يعد موضوع مكافحة جرائم الإرهاب الإلكتروني من الموضوعات الهامة والحيوية، وعلى الرغم من وجود العديد من الدراسات السابقة التي تناولت موضوع جرائم الإرهاب الإلكتروني، إلا أنه لا توجد أي دراسة تناولت دور الذكاء الاصطناعي في التصدي لجرائم الإرهاب الإلكتروني، من خلال التطرق لتشريعات والأنظمة القانونية في المملكة العربية السعودية للتصدي لجرائم الإرهاب الإلكتروني، لذلك تختلف الدراسة الحالية عن الدراسات السابقة في أنها تطرقت لبيان دور الذكاء الاصطناعي في التصدي لجرائم الإرهاب الإلكتروني، ومن خلال التعرض للبنيان القانوني والاتفاقيات التي انضمت إلى المملكة العربية السعودية بهذا الشأن، وبذلك تصبح الدراسة الحالية أعم وأشمل من الدراسات السابقة.

وندكر على سبيل المثال لا الحصر من الدراسات السابقة البحث الموسوم ب (تطبيقات الذكاء الاصطناعي في مواجهة الجرائم الالكترونية للباحث علي احمد ابراهيم-المجلة القانونية ص 2810-2836)، وكذلك البحث المعنون ب (دور الذكاء الاصطناعي في مواجهة الجرائم الإلكترونية للباحثين الخضر دولي ونفيسة ناصري، مجلة المؤشر للدراسات الاقتصادية 2018) وغير ذلك كثير.

8.1 خطة الدراسة

تنقسم خطة الدراسة إلى ثلاثة مباحث رئيسة يسبقها مقدمة وتنتهي بخاتمة، على النحو التالي:

- المبحث الأول: ماهية الذكاء الاصطناعي ودوره في مواجهة جرائم الإرهاب الإلكتروني.
- المبحث الثاني: التنظيم القانوني لجرائم الإرهاب الإلكتروني.
- المبحث الثالث: موقف التشريعات والاتفاقيات العربية من مواجهة جرائم الإرهاب الإلكتروني.

2. المبحث الأول: ماهية الذكاء الاصطناعي ودوره في مواجهة جرائم الإرهاب الإلكتروني:

يعد الذكاء الاصطناعي سلاحًا ذو حدين، إيجابيًا في تتبع وتعقب الجرائم والمجرمين وسلبيًا في استخدام الإرهابيين لأنظمة الذكاء الاصطناعي في ارتكاب جرائمهم الإرهابية بما سمح لهم باستخدام بيانات ضخمة وتحليلها عبر الإنترنت بغرض تسهيل عملياتهم الإرهابية، والتجنيد الإلكتروني للشباب من خلال الشبكة العنكبوتية. لذلك سينقسم هذا المبحث إلى المطلبين التاليتين: المطلب الأول ماهية الذكاء الاصطناعي، والمطلب الثاني دور أنظمة الذكاء الاصطناعي في مواجهة جرائم الإرهاب الإلكتروني.

1.2 المطلب الأول: ماهية الذكاء الاصطناعي:

يعد الذكاء الاصطناعي فرع من فروع علم الحاسوب فهو محاكاة لذكاء الإنسان عبر أنظمة التقنية من خلال جمع البيانات وتحليلها واتخاذ القرارات بناء على عملية تحليلية بصورة تحاكي طريقة تفكير البشر. ويتميز الذكاء الاصطناعي بقدره على جمع المعلومات وتحليلها، الأمر الذي يمكنه من اكتساب خبرات من المواقف التي يحفظها، والتي تؤهله وتجعله يتخذ قرارات مستقلة وذاتية. ويهدف الذكاء الاصطناعي إلى فهم طبيعة الذكاء الإنساني، عن طريق إنشاء تطبيقات متخصصة قادرة على محاكاة السلوك الإنساني المتسم بالذكاء، فتلك التقنيات تفكر، وتستنتج وتعطي الحلول، وبل تتنبأ بالمستقبل (عبير مُحَمَّد أسعد، 2017م، ص 3 وما بعدها).

1.1.2 الفرع الأول: مفهوم الذكاء الاصطناعي:

يعرف الذكاء الاصطناعي على أنه: "مجموعة من السلوكيات التي تتسم بها البرامج الحاسوبية، ويكون الهدف منها تقوية القدرة الإنتاجية من جهة والعمل على محاكاة

القدرات الذهنية البشرية من جهة أخرى". ويعرف البعض بأنه: مجموعة من السلوكيات التي تتسم بها البرامج الحاسوبية، ويكون الهدف منها تقوية القدرة الإنتاجية من جهة، والعمل على محاكاة القدرة الذهنية البشرية من جهة أخرى، وهذا أمر تم اتقانه، وأصبح الجميع على علم به حتى يومنا هذا، فقد استطاع الذكاء الاصطناعي أن يغزو جميع الأجهزة الخاصة بنا، حتى أصبحت الملاذ الأمن للعديد من الأشخاص، وكان لا بد من إيجاد الوسيلة الفاعلة من أجل التعامل الجاد مع هذه البرامج بما يحقق القدرة الإنتاجية، والتعامل الإيجابي بين الإنسان والآلة على حد سواء. ويمكن الذكاء الاصطناعي الإنسان من استخدام اللغة الإنسانية في التعامل مع الآلات عوضاً عن لغات البرمجة الحاسوبية مما يجعل الآلات واستخدامها ما في متناول كل شرائح المجتمع. ويساهم الذكاء الاصطناعي في اتخاذ القرارات بعيدة عن الخطأ والانحياز والعنصرية. ويهدف الذكاء الاصطناعي لايجاد نظم تفكر مثل البشر، وتحلل البيانات بشكل منطقي. (وجيه مُحَمَّد سليمان،2022م، ص 455 – 456).

يتضح لنا مما سبق، أن الذكاء الاصطناعي هو محاكاة لطرق ذكاء الإنسان ومحاكاة لكيفية استخدام خبرته المكتسبة في مجال معين وكذلك طرق تفهمه للغات المختلفة وكيفية التعرف على الصور والتحدث والتي أدت إلى تطور وظهور تقنيات لتصميم برامج تحول الحاسوب إلى آلات تعمل أعمالاً تتسم بالذكاء والخبرة الإنسانية المكتسبة أو آلات ذات ذكاء مصنع.

ويمكن تعريف الذكاء الاصطناعي على أنه: مجموعة من الأساليب والطرق الجديدة في برمجة الأنظمة والتي يمكن أن تستخدم لتطوير أنظمة تحاكي بعض عناصر ذكاء الإنسان وتسمح لها بالقيام بعمليات استنتاجية عن حقائق وقوانين يتم تمثيلها في ذاكرة الحاسب، ولا يمكن أن نقول بأن الذكاء الصناعي هو برامج الكمبيوتر التي تحاكي طريقة تفكير البشر، حيث إن العلماء في هذا المجال لم يتمكنوا من الوصول إلى ذلك حتى الآن. (علي أحمد إبراهيم، 2021، ص 2815)

2.1.2 الفرع الثاني: خصائص الذكاء الاصطناعي:

تعتبر الذكاء الاصطناعي محاكاة للذكاء البشري من خلال التطبيقات الحديثة وأجهزة الحاسوب، لذلك يجب توفر عدة خصائص الذكاء الاصطناعي وهي:-

- اكتساب المعلومات من خلال مواقف جديدة ومتغيرة، ووضع قواعد لهذه المعلومات، وتكون هذه القواعد على شكل نماذج مخزنة في النظام الذكي.
- قدرة الذكاء الاصطناعي على اتخاذ القرار باستقلالية دون تدخل بشري، أي أن يكون قرار هذا النظام بناء على البيانات المحصلة، وعليه يكون مستقل عن الإرادة البشرية، أي بدون تحكم من البشر.
- قدرة الذكاء الاصطناعي على تحليل البيانات وجمع المعلومات وإمكانية إيجاد علاقات فيما بينها الأمر الذي يؤدي إلى الانتشار المتزايد للبيانات العملاقة.
- قدرة الذكاء الاصطناعي على التكيف مع البيئة المحيطة والتسبيب والاستنباط، بحيث تكون قرارات الذكاء الاصطناعي مبنية على الاستنباط من الظروف البيئية المحيطة. (علي أحمد إبراهيم، 2021، ص 2816)

3.1.2 الفرع الثالث: أنواع الذكاء الاصطناعي:

أدى التطور الهائل لأنظمة الذكاء الاصطناعي إلى ظهور تصنيفات للذكاء الاصطناعي من حيث رد الفعل البسيط إلى الإدراك والتفاعل الذاتي، وهي النحو التالي:

- أولاً:- الذكاء الاصطناعي الضيق: وهو أبسط أنواع الذكاء الاصطناعي والذي تتم برمجته للقيام بوظائف معينة داخل بيئة محدودة، ولا يمكنه العمل إلا في الإطار المحدد له.
- ثانياً:- الذكاء الاصطناعي العام: وهو الذي يتميز بالقدرة على جمع المعلومات والعمل على تحليلها، الأمر الذي يمكنه من اكتساب خبرات من المواقف التي يحفظها، والتي تؤهله وتجعله يتخذ قرارات مستقلة وذاتية.
- ثالثاً:- الذكاء الاصطناعي الخارق: ويعتبر هذا النوع من النماذج التي لا تزال تحت التجربة، وهي تتطور مع تطور عصر التكنولوجيا، والتي تسعى لمحاكاة الإنسان، ويمكن التمييز بين نمطين منها الأول يحاول فهم الأفكار البشرية والانفعالات والتي تؤثر على سلوك الإنسان، أما النوع الثاني فهو نموذج لنظرية العقل، والتي لها القدرة على التعبير عن حالاتها الداخلية، والتنبؤ بمواقف الآخرين ومشاعرهم وتتفاعل معها، فالإنسان قادر على أن يأتي بأنواع مختلفة من العمليات الذهنية مثل الاختراع والاستنتاج بكافة أنواعه في حين أن الأنظمة الذكية تقتصر على استنتاجات محدودة طبقاً لبديهيات وقوانين متعارف عليها يتم برمجتها في البرامج نفسها على هذا الأساس. (وجيه مُحَمَّد سليمان،2022م، ص 458)

2.2 المطلب الثاني: دور أنظمة الذكاء الاصطناعي في مواجهة جرائم الإرهاب الإلكتروني:

يجب الربط بين التكنولوجيا والقانون، وذلك من خلال الإطار القانوني النظري والتطبيق العملي لتكنولوجيا الحديثة كالذكاء الاصطناعي، وهذا يستدعي بالضرورة مواكبة التشريع الجنائي للتطور التقني لتطبيق القواعد القانونية على أنظمة الذكاء الاصطناعي، فللذكاء الاصطناعي له دور كبير في التحري والتحقيق في جرائم الإرهاب الإلكتروني ومواجهته في ظل اعتماد الجماعات الإرهابية في ارتكاب جرائمهم على أسلوب تقني ومتطور ومبتكر، لذلك كان لا بد من دمج تقنيات الذكاء الاصطناعي في مجال التحقيق الجنائي في جرائم الإرهاب الإلكتروني من خلال اختراق الأنظمة المعلوماتية كمراقبة الاتصالات وحسابات التواصل الاجتماعي لاكتشاف الجرائم الإرهابية قبل وقوعها والتنبؤ بحدوثها(وجيه مُحَمَّد سليمان،2022م، ص 464).

1.2.2 الفرع الأول: الاعتراض على الرسائل الإلكترونية:

تعتبر وسيلة مراقبة المكالمات والرسائل الإلكترونية للمتهمين أو المشتبه بهم من الوسائل التقنية التي تحتاج إلى أنظمة ذكية لتحقيق الغاية المرجوة منها، كوجود أنظمة الذكاء الاصطناعي التي لها القدرة على اعتراض المكالمات وتحديد علاقة المتهم بالجريمة.

ويقصد بالاعتراض: هو مراقبة الرسائل المرسلة بأي شكل من الأشكال بوسيلة الإلكترونية عن طريق التقاط الموجات الكهربائية، فيكون الاعتراض بجمع البيانات المرسلة وتحويلها إلى معلومات مقروءة، أو مسجلة دون تحديد المعلومات المراد استخراجها، وإنما يكون الاعتراض على جميع البيانات المرسلة ليتم استخلاص المعلومات التي لها علاقة بارتكاب الجريمة بعد معالجتها وتحويلها بصورة تسمح بمعرفة فحواها وإعدادها لتصبح دليلًا على صاحبها (وجيه مُحَمَّد سليمان، مرجع سابق، ص 466).

وحيث أجاز القانون إمكانية اعتراض الرسائل والمراسلات الإلكترونية متى ما كان هذا في مصلحة التحقيق، والاعتراض هنا يشمل جميع المراسلات الإلكترونية بما في ذلك من الاتصالات الهاتفية أو مراسلات إلكترونية كالبريد الإلكتروني. ولهذه الرسائل الإلكترونية أهمية وفائدة في كشف الحقائق التي تتعلق بارتكاب جرائم الإرهاب.

2.2.2 الفرع الثاني: تطبيقات الذكاء الاصطناعي للتنبؤ بجرائم الإرهاب الإلكتروني:

تساعد تطبيقات الذكاء الاصطناعي في الكشف عن الجرائم المتوقع حدوثها في المستقبل، وبمدة كافية لتمكن السلطة المختصة بمكافحة هذه الجرائم بمنعها قبل ارتكابها، وذلك من خلال تحليل البيانات الضخمة، وربط بعضها ببعض، وإعطاء النتائج، يسمي ذلك بالتنبؤ الخوارزمي للجرائم. وتعد الخوارزميات هي الأداة التي تستخدمها آلات الذكاء الاصطناعي في التنبؤ بالجريمة، وتعني الخوارزميات: بأنها مجموعة من المسارات والخطوات الرياضية المتتابعة المتتالية اللازمة لحل مشكلة ما، والمعدة برمجيا لكي تعطي نتيجة معينة اعتماداً على معطيات ومدخلات غذيت بها. ويوجد العديد من مصادر البيانات الضخمة، إذ تُعد هي الوسيلة التي يتم استخدامها بواسطة الخوارزميات، لمسح، وتصفية، وفهم، وتحليل، وفرز، ومعالجة البيانات، فكلما تضخّمت البيانات سهُل التوقّع، فكلما ازدادت المعلومات أصبح بالقطع أكثر إدراكًا وقُدرة على اتخاذ القرار الملائم (محمود سلامة الشريف، 2021م، ص 342). ومنها المصادر التقنية معتمدة على شبكات أجهزة التتبع، كالتصوير بالأقمار الاصطناعية، وتتبع البيانات المستمدة من الهواتف المحمولة والنظام العالمي لتحديد المواقع GPS غيرها. وهناك نوع آخر من المصادر وهو المتعلق بسلوك المجرم مثل مرات البحث على الإنترنت عن كيفية تصنيع متفجرات أو أي نوع آخر من المعلومات، ومرات مشاهدة إحدى الصفحات المشبوهة على الإنترنت. وأخيرًا، مصادر البيانات المتعلقة بالآراء مثل التعليقات المجرم بتحريض على العنف ضد الدولة على وسائط التواصل الاجتماعي، مثل فيسبوك وتويتر وغيرها.

ومن أشهر تطبيقات الذكاء الاصطناعي هو [PredpoI]، والذي يستشعر أماكن الخطر التي يُزمع ارتكاب الجرائم فيها، كذلك التنبؤ بمرتكبيها من خلال تحليل كم هائل من البيانات والصور والفيديوهات، وغيرها – مثل المعلومات المتعلقة بوسائل التواصل الاجتماعي للشخص، ومعلومات الحي الذي يقطن به، والصحيفة الجنائية. إذ تمثل تلك البيانات الأداة التي تمكّن التطبيق من إعطاء المؤشرات التي ترنو إلى تحديد نسبة احتمال ارتكابه جريمة معينة (عبير مُحَمَّد أسعد، مرجع سابق، ص 18 وما بعدها). ويمكن استغلال قدرات تطبيقات الذكاء الاصطناعي على تحليل الفيديوهات والصور في كشف الهجمات الإرهابية. ومن بين تلك التطبيقات كاميرات IP من خلال نشرها في جميع أنحاء الأماكن الحيوية، لضبط مراقبة البث المباشر للأنشطة غير القانونية التي تسجلها الكاميرات. تتميز هذه الكاميرات بنظام التعرف على الوجه الذي يطابق أوجه الأشخاص الذين أمام الكاميرا بالأشخاص

المدرجين في القائمة السوداء لدى القوات الأمنية والمخزنين مسبقا في قاعدة بيانات على نظام الكاميرا، وبفور التعرف على وجه المشتبه به يطلق إنذارا في محطة المراقبة (عبد الله موسي، وأحمد حبيب، 2019م، ص 98). ومن أهم تطبيقات الذكاء الاصطناعي التي تستخدم لتحديد الأشخاص الانتحاريين الذين يرتدون المتفجرات تحت ملابسهم، هو جهاز تصوير الأشعة لكشف ما وراء الملابس وهو يستخدم أشعة تيراهيرتز (Terahertz) لاكتشاف وتصوير وتحديد الأسلحة المخبأة مع الشخص المشتبه به، إضافة لنظام التعرف على الوجوه والذي يوفر مرونة في معرفة المجرمين ويمكن استخدامه في نقاط التفتيش الأمنية والمطارات والمنافذ المختلفة (عمرو سيد البحيري، 2019م، ص 13).

3.2.2 الفرع الثالث: التحقيق الجنائي الرقمي في جرائم الإرهاب الإلكتروني:

تساعد أنظمة الذكاء الاصطناعي جهة التحقيق في جرائم الإرهاب الإلكتروني على التعرف على هوية الشخص أو مرتكب الجريمة من خلال اسم المستخدم الخاص به، أو الرسائل الإلكترونية الخاصة به، أو من خلال رقم هاتفه، التي تم التوصل إليها بالتحقيق، لذلك أصبحت وسيلة من وسائل الإثبات الجنائي وهي عن طريق استخراج تلك البيانات والمعلومات لما لها من أهمية والقوة في الإثبات وتكون حجة على مرتكبها، الأمر الذي يتطلب من المحققين الاهتمام في كيفية استخراج تلك الأدلة والاهتمام بها وكيفية تحديد هوية الفاعل (محمود سلامة الشريف، مرجع سابق، ص 346).

وتسعي العديد من دول العالم إلى تحول حكومتها بالكامل إلى حكومات رقمية، وأول خطوة هي تفعيل الهوية الرقمية، حيث إن وجود الهوية الحقيقية للشخص بإعطاء نسخة رقمية عن هوية الدولة أو رخصة القيادة أو أي أوراق ثبوتية أخرى، تساعد المحققين في كشف مرتكبي جرائم الإرهاب. ويتم الاعتماد على شبكة الإنترنت في رفع الملفات الرقمية للقضايا التي تحتوي على أدلة جنائية، كسجلات المتهمين وكافة الإجراءات المتخذة قبلهم من محاضر وتحقيقات وأحكام سابقة، لإتاحة استخدامها من قبل العديد من المحققين في الجرائم المختلفة (وجيه مُحَمَّد سليمان، مرجع سابق، ص 469 وما بعدها).

وتعتمد جهات التحقيق في الدول المتقدمة على تقنية بصمة المخ والتي تستخدم في عمليات مسح دماغ المشتبه به عند استجوابه من قبل المحقق، ويحدد ما إذا كان الشخص الذي يجري التحقيق معه يتذكر معلومات معينة عن الجريمة المطلوبة بسببها، ومن ثم التأكد من تحديد علاقة المشتبه به بالجريمة استنادًا إلى نتائج المسح الفوري. وتختلف تقنية بصمة المخ عن جهاز كشف الكذب، حيث إن النظام القائم عليه جهاز كشف الكذب هو استجابة الضغط العصبي، حيث إن الشخص الذي يكذب يزداد قلقه فضلاً عن تغييرات عاطفية أخرى، أما النظام القائم عليه تقنية بصمة المخ هو استجابة المخ والذي يقوم بالتحقيق في المعلومات الموجودة في المخ والكشف عنها بأسلوب خال من الضغط العصبي، والتأكد من وجود هذه المعلومات التي تثبت أو تنفي الجريمة ويكون محلها في المخ (محمود سلامة الشريف، مرجع سابق، ص 350، 351).

وجدير بالذكر أن تقييم الخطورة الإجرامية للمتهم، واحتمالية ارتكابه لجريمة تالية يتحقق أيضًا من خلال خوارزميات التنبؤ بالجريمة، وتعطي - اعتمادًا على بيانات معينة – مؤشرًا إلى مدى الخطورة الإجرامية لشخص ما، بل ويُعتد بهذا التقييم في مراحل الإجراءات الجنائية المختلفة، ولعلّ تطبيق كومباس "COMPASS" من أهم التطبيقات التي تحدد موقع الشخص من الخطورة الإجرامية. والذي يضطلع بقياس وتقييم درجة الخطورة الإجرامية لشخص ما اعتمادًا على خوارزميات تقنية تقوم بتحليل بياناته الشخصية (عمرو سيد البحيري، مرجع سابق، ص 25).

وجدير بالإشارة أنه، تؤكد دولة الإمارات العربية المتحدة على الاعتماد على استراتيجية الذكاء الاصطناعي في الخدمات وتحليل البيانات بمعدل ١٠٠ % بحلول عام ٢٠٣١م، واستحداث وزارة للذكاء الاصطناعي، كما هو في المملكة العربية السعودية وجمهورية مصر العربية، والتي تستهدف تطوير الأداء الحكومي إلى مستويات غير مسبوقة إضافة إلى تسريع الإنجاز وتأسيس بيئات عمل مبدعة ومبتكرة ذات إنتاجية عالية، وتبني حكومة دولة الإمارات أفضل وأحدث التطبيقات في تقنية المعلومات لخلق الحكومة المتميزة على مستوى العالم، وقد سبقتها المرحلة الأولى التي دشنت الحكومة الإلكترونية ثم المرحلة الثانية التي جاءت بالحكومة الذكية. وإستراتيجية الذكاء الاصطناعي هي بأكورة المشاريع الضخمة التي تم الإعلان عنها ضمن مئوية الإمارات ٢٠٧١م، وسيتم من خلالها توجيه الاستثمارات نحو أحدث تقنيات الذكاء الاصطناعي وتطبيقها في شتى ميادين العمل في الدولة بكفاءة رفيعة المستوى، إضافة إلى استثمار الموارد والإمكانات البشرية والمادية المتوافرة بطريقة مبدعة. وستركز حكومة الإمارات على تسخير مقومات ومزايا الذكاء الاصطناعي في مختلف القطاعات (علي أحمد إبراهيم، 2021، ص2826).

3. المبحث الثاني: التنظيم القانوني للجرائم الإرهاب الإلكتروني:

أدي ظهور التكنولوجيا الحديثة وثورة الاتصالات والمعلومات، إلى تفاقم ظاهرة الإرهاب الإلكتروني، فلم يعد يحتاج الإرهابي سوى جهاز حاسوب آلي متصل بشبكة الإنترنت للقيام بالعمليات الإرهابية. فأصبحت جريمة الإرهاب الإلكتروني وصوره خطر يهدد العالم بأسره، ويكمن الخطر فيها في سهولة استخدام الجماعات الإرهابية لوسائل الاتصالات الإلكترونية في تسهيل الاتصال بين أعضائهم، أو التجنيد الأشخاص الجدد، أو نشر وترويج لأفكارهم ومبادئهم، والتنظيم للمخططات الإرهابية، أو التدريب على تصنيع المتفجرات، أو استغلال الشبكة المعلوماتية في تمويل الإرهاب. لذلك سينقسم هذا المبحث إلى المطالب التالية: المطلب الأول أركان جرائم الإرهاب الإلكتروني، والمطلب الثاني صور جرائم الإرهاب الإلكتروني، والمطلب الثالث وسائل الإرهاب الإلكتروني.

1.3 المطلب الأول: أركان جرائم الإرهاب الإلكتروني:

لا تختلف أركان جريمة الإرهاب الإلكتروني عن أركان أي جريمة الإرهاب تقليدية، ألا من حيث الوسيلة والأداة الإجرامية التي تستخدم في ارتكابها، لذلك لابد من توافر شرط خاص مفترض في هذه الجرائم بجانب الأركان العامة للجريمة وهي الركن المادي، والركن المعنوي، بإضافة للشرط المفترض وهو وقوع الجريمة الإرهابية بواسطة استخدام إحدى وسائل تقنيات المعلومات، لهذا تمثل وسائل تقنية المعلومات ركناً مفترضاً في هذه الجريمة، يترتب على عدم توافره انتفاء صفة التجريم عن الفعل، فبالتالي تكون جريمة مستحيلة، وذلك لانعدام محل الفعل، وإن كان ذلك لا يمنع من أن يُشكل الفعل وصفاً تجريمياً آخر. وفي ضوء ما سبق سنتناول الأركان العامة للجريمة من خلال الفروع التالية:

1.1.3 الفرع الأول: الركن المادي:

يعد الركن المادي للجريمة هو السلوك الصادر من الجاني ويحدث أثر في العالم الخارجي ويعاقب عليه القانون، وهو نوعان: إما سلوكاً سلبياً أو سلوكاً إيجابياً، فالأول يتحقق في حالة الامتناع عن فعل يأمر عليه القانون، أما الثاني هو القيام بفعل يجرمه القانون ويؤدي إلى إحداث نتيجة في الجرائم ذات النتيجة، ولا يعتد القانون بالوسيلة المستعملة سواء كانت مادية أو معنوية في ارتكاب السلوك الإجرامي. ويتمثل الركن المادي للجريمة في سلوك إرادي يترتب عليه نتيجة إجرامية تربطها بالسلوك الإجرامي رابطة سببية مادية، ويتكون الركن المادي في جريمة الإرهاب الإلكتروني من ثلاثة عناصر رئيسية وهما: السلوك الإجرامي، والنتيجة الإجرامية والعلاقة السببية.

1.1.1.3 السلوك الإجرامي

يقصد بالسلوك الإجرامي: هو النشاط المادي الخارجي الذي يصدر عن الجاني ليحقق النتيجة الإجرامية التي يعاقب عليها القانون، لابد من توفره لوقوع الجريمة سواء كان سلوكًا إيجابيًا أم سلبيًا، وأننا نري أنه، تعد جرائم الإرهاب الإلكتروني من الجرائم الإيجابية ويتمثل ذلك في النشاط الإرادي الخارجي الذي يستخدم فيه الجاني أعضاء جسمه لإحداث الأثر الخارجي المحسوس للسلوك مكونًا لماديات الجريمة ومسببًا لما قد يترتب عليها من ضرر أو خطر، ولم يشترط حتى تقوم هذه الجريمة أن ينتج عن فعل استخدام نظام المعلوماتي أو الشبكة المعلوماتية في إنشاء موقع لتسهيل الاتصال بين أعضاء المنظمة، أو القيام بأعمال إرهابية، أو نشر وترويج لأفكارهم المتطرفة بالفعل، وإنما يكفي أن يكون قصد الجاني قد اتجه إلى ذلك، وليس بالضرورة أن يؤدي استخدام الشبكة المعلوماتية إلى تعريض المواطنين أو ممتلكاتهم لخطر أعمال عدائية تقع عليهم، أو على أموالهم، بل يكفي احتمال تحقق ذلك وهذا ما يسمى بجرائم الخطر(باسل فايز حمد، 2019م، ص 32وما بعدها؛ زين العابدين عواد كاظم الكردي، 2018م، ص 88 وما بعدها).

وأن من أهم ما يميز جرائم الإرهاب الإلكتروني بشكل عام هو وجود جهاز حاسب آلي أو أي جهاز إلكتروني متصل بشبكة الإنترنت، فبدون هذه الأجهزة الإلكترونية لا يمكننا تصور وجود جريمة الإرهاب الإلكتروني، فمثلًا كجريمة إنشاء موقع لمنظمة إرهابية لتسهيل الاتصال بين أعضائها، أو نشر وترويج أفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة المتفجرات، أو أي أداة تستخدم في الأعمال الإرهابية على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي، وجريمة الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي ، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الدولة الداخلي أو الخارجي، أو اقتصادها الوطني. فالسلوك الإجرامي له صورة متعددة وتختلف باختلاف نوع الجريمة المرتكبة، ففي جرائم الإرهاب الإلكتروني لابد من قيام الجاني بممارسة نشاط تقني باستخدام جهاز الحاسب الآلي أو أي جهاز إلكتروني متصل بشبكة الإنترنت في بيئة رقمية. مثال ذلك: كاستخدام تقنية الريموت كنترول في التفجير عن بعد، أو جوجل إيرث في تحديد ورصد تحركات المجني عليهم.

2.1.1.3 النتيجة الإجرامية:

تُعرّف النتيجة الإجرامية بأنها هي: "الأثر القانوني المترتب على السلوك الإجرامي للجريمة"، فهو الأثر الخارجي الذي يتولد عن هذا السلوك، فيتمثل في النتيجة التي توصل إليها الجاني، وتعتبر جريمة الإرهاب الإلكتروني من حيث النتيجة من جرائم الخطر، فيفترض المشرع فيها الخطر المتمثل بنتيجتها وهو تسهيل الاتصال بين قيادات وأعضاء المنظمات، أو نشر وترويج الفكر الإرهابي، أو تمويله، أو نشر أساليب التدريب، أو تصنيع الأجهزة الحارقة، أو المتفجرات، فبمجرد قيام الجاني بالسلوك الخارجي المحددة بنصوص القانون تقوم الجريمة ويتم العقاب عليها، وهذا من حيث الفعل المكون للجريمة، والتي لم يشترط المشرع فيها تحقيق النتيجة. مثال ذلك: كإنشاء موقع إلكتروني لمنظمة إرهابية لتسهيل الاتصال بقيادات وأعضائها، أو لنشر وترويج أفكارها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات، أو نشر أساليب التدريب، فتقوم الجريمة بغض النظر عن تحقيق الاتصال بين قيادات وأعضاء المنظمة الإرهابية أو فشله، أو وجود أي مستخدمين على الشبكة المعلوماتية أو رؤيتهم للموقع الإلكتروني، ومن ثم يُعد فعل الإنشاء في حد ذاته كافياً لتحقيق الجريمة، كذلك في جريمة الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الدولة الداخلي أو الخارجي، أو اقتصادها الوطني، فتقوم الجريمة بغض النظر عن حصول الجاني على بيانات تمس الأمن الدولة الداخلي أو الخارجي، أو اقتصادها القومي أم عدمه، لأنها من جرائم الخطر التي يندمج فيها السلوك مع النتيجة، فلا يشترط فيها الضرر الفعلي، لأنها تمس أمن الدولة واقتصادها(مُحَمَّد علي سويلم، 2018م، ص 45 وما بعدها؛ بدره هويمل الزين، 2012م، ص 76 وما بعدها).

3.1.1.3 العلاقة السببية:

تُعرف العلاقة السببية بأنها هي:"العلاقة بين السلوك الإجرامي للجاني وبين النتيجة الإجرامية"، بمعنى أن السلوك الإجرامي هو السبب في إحداث النتيجة الإجرامية، ولولا هذا السلوك ما كانت لتحدث النتيجة الإجرامية، لذلك حتى تكتمل جميع عناصر الركن المادي للجريمة لابد من وجود علاقة سببية تربط بين السلوك الإجرامي وما تحققه من نتيجة إجرامية، فإذا انتفت العلاقة السببية التي تربط بين السلوك الإجرامي والنتيجة الإجرامية انتفت المسؤولية الجنائية.

وأننا نري أنه، لا يشترط في جريمة الإرهاب الإلكتروني العلاقة السببية، أي أنه لا يشترط فيها نسب السلوك إلى الجاني، لأنها من جرائم الخطر فلا يشترط لاكتمال الجريمة تحقيق النتيجة الإجرامية. وتنعقد المسؤولية الجنائية بمجرد إنشاء موقع إلكتروني أو صفحة شخصية، لاستخدامها في تسهيل الاتصال بين قيادات وأعضاء المنظمات، أو نشر وترويج الأفكار الإرهابية، أو تمويله، أو نشر أساليب تصنيع المتفجرات أو أي أدوات تستخدم في الإرهاب. وكذلك في جريمة التجسس الإلكتروني فبمجرد الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الدولة الداخلي أو الخارجي، أو اقتصادها الوطني.

2.1.3 الفرع الثاني: الركن المعنوي:

يتكون القصد الجنائي للجريمة الإرهاب الإلكتروني من عنصري العلم والإرادة كسائر الجرائم العادية، لذلك لابد أن يعلم الجاني بأن سلوكه يمثل جريمة، مع اتجاه إرادته إلي ارتكاب الفعل المجرّم، وينفي القصد الجنائي لدي الجاني عندما يكون الدخول إلى الموقع الإلكتروني عن طريق الخطأ، وبالتالي تنتفي المسؤولية الجنائية.

وتعتبر جريمة الإرهاب الإلكتروني من الجرائم العمدية والتي يلزم لتحققها توافر القصد الجنائي بشقيه العلم والإرادة، فلا يمكن أن تقع عن طريق الخطأ غير العمدي، والقصد الجنائي المتطلب لقيام هذه الجريمة هو القصد الجنائي العام المتمثل في علم الجاني بموضوع الجريمة وقت ارتكاب فعله، أي أن يكون الجاني علمًا بحقيقة الواقعة الإجرامية أثناء مباشرته للنشاط الإرهابي، بأنه ينشئ موقعًا إلكترونيًا لصالح منظمة إرهابية، بغرض تسهيل الاتصال بين قياداتها وأعضائها، أو نشر وترويج أفكارها الإرهابية، أو تمويلها، أو نشر أساليب تصنيع المتفجرات أو أي أدوات تستخدم في الإرهاب، ويجب أن تتجه إرادة الجاني إلى تحقيق النتيجة الإجرامية المتمثلة في تسهيل الاتصال بين قياداتها وأعضائها، أو نشر وترويج الأفكار الإرهابية، أو تمويلها، أو نشر أساليب تصنيع المتفجرات أو أي أدوات تستخدم في الأعمال الإرهابية. وكذلك في جريمة التجسس الإلكتروني لابد أن الجاني علماً بأن هذا الموقع الإلكتروني يوجد بها بيانات تمس الأمن الدولة الداخلي أو الخارجي، أو اقتصادها الوطني. ويجب أن تتجه إرادة الجاني إلى تحقيق النتيجة الإجرامية المتمثلة في الحصول على هذه البيانات، ولكن مجرد الدخول إلى الموقع الإلكتروني أو النظام المعلوماتي، أو الحاسب الآلي لأي غرض آخر غير الحصول على هذه البيانات ينفي عنصر العلم، ومن ثم ينفي القصد الجنائي. مثال ذلك: كالدخول إلى

الموقع الإلكتروني مصادفة وظهرت فيه البيانات أمام الشخص عند استخدامه الموقع الإلكتروني أو النظام المعلوماتي، أو الحاسب الآلي دون سعي منه للحصول عليها، حتى لو اطلع عليها بطريق الخطأ، أنه إذا قام بإفشائها للغير فتنعقد المسؤولية الجنائية عن الجريمة في حقه (خالد حامد مصطفي، 2016م، ص 120 وما بعدها).

2.3 المطلب الثاني: صور جرائم الإرهاب الإلكتروني

ساهم التطور الهائل في ثورة الاتصالات والمعلومات على استخدام الجماعات الإرهابية للمواقع والصفحات الإلكترونية لتسهيل الاتصال بين قياداتها وأعضائها، أو لاستقطاب المراهقين والشباب من مختلف دول العالم لتجنيدهم وانضمامهم لهذه الجماعات الإرهابية، أو نشر وترويج لأفكارها، أو تمويل عملياتها الإرهابية، أو التجسس الإلكتروني على الدول. وتتعدد صور جرائم الإرهاب التي ترتكب باستخدام تقنية المعلومات. ولذلك سنتناول في هذا المطلب أكثر صور جرائم الإرهاب الإلكتروني انتشارًا من خلال الفروع التالية:

1.2.3 الفرع الأول: جريمة التجنيد للتنظيمات الإرهابية:

يعد تجنيد الأفراد عبر شبكة الإنترنت من بين أخطر صور الإرهاب الإلكتروني، حيث تحاول الجماعات الإرهابية الاستفادة من ثورة الاتصالات في التواصل والتنسيق فيما بينها، وإخفاء عملياتها بطرق جديدة، ويمكن استخدام مواقع التواصل الاجتماعي في التواصل مع الراغبين إلى الانضمام في صفوف المنظمات الإرهابية، وتجنيدهم واقناعهم في تبني أفكارها وتسهيل مهمة انتقالهم من أماكن تواجدهم إلى ساحات القتال، ونشر الخطاب المتطرف والحث على العنف من خلال الاستخدام السيء لمواقع التواصل الاجتماعي من جانب الإرهابيين للترويج إلى أفكارهم حيث تسهيل هذه المواقع على انتشار الأفكار المتطرفة بين مختلف الطبقات الاجتماعية خصوصاً الطبقات الفقيرة والقصر والعاطلين عن العمل (إيمان بن سالم، 2018م، ص 37).

2.2.3 الفرع الثاني: جريمة الترويج للتنظيمات الإرهابية:

تستخدم الجماعات الإرهابية شبكة الإنترنت في نشر ثقافة الإرهاب والترويج لها، وكما تسعى جاهدة إلى توفير أكبر عدد ممكن من الراغبين في تبني أفكارها ومبادئها، ويمكن ارتكاب جريمة الترويج للتنظيمات الإرهابية من خلال الشبكة العنكبوتية بحيث يتم إرسال رسائل من خلال البريد الإلكتروني وشبكات التواصل الاجتماعي للتواصل بين الإرهابيين وتبادل المعلومات فيما بينهم، وتناقلها بين القائمين بالعمليات الإرهابية والمخططين لها، والاستفادة منه في نشر أفكارهم والترويج لها والسعي لزيادة الأتباع والمتعاطفين معهم عبر الرسائل الإلكترونية(خالد حسن لطفي، 2018م، ص 115 وما بعدها).

3.2.3 الفرع الثالث: جريمة تمويل التنظيمات الإرهابية:

تستخدم التنظيمات الإرهابية الشبكة العنكبوتية في تمويل العمليات الإرهابية عن طريق جمع التبرعات من خلال الجمعيات الخيرية حيث إن معظم التنظيمات الإرهابية تقوم بإنشاء شركات وهمية تحت غطاء منظمات خيرية تهدف إلى جمع الأموال والتبرعات لخدمة مجال معين، ولكنها تقوم بتحويل الأموال التي تحصل عليها إلى الجماعات الإرهابية.

وترتبط جريمتي غسيل الأموال وتمويل الإرهاب بارتباط وثيق، وذلك من خلال الهدف الأساسي والمرجو من كلتا الجريمتين والمتمثل بإخفاء المصدر والأصل الحقيقي غير المشروع للأموال، بشأن تجريم تمويل الأعمال الإرهابية، أن نظرة المجتمع الدولي لتمويل الإرهاب هي ذات النظرة التي تكافح جريمة غسيل الأموال نظرًا للارتباط الوثيق من خلال الغاية لكل منها(عبدالله سعد محدي، 2018م، ص 66).

4.2.3 الفرع الرابع: جريمة التجسس الإلكتروني:

تستخدم التنظيمات الإرهابية الشبكة المعلوماتية في التجسس على الدول أو المنظمات أو المؤسسات الدولية أو الوطنية، وقد تحولت وسائل التجسس من الطرق التقليدية إلى الطرق الإلكترونية خاصة مع ظهور الشبكة المعلوماتية، فإن حدود الدولة كالمواقع العسكرية وأنظمة التسليح والتي تمس الأمن القومي، بحيث تكون تلك البيانات مستباحة بأقمار التجسس والبث الفضائي، ولا يشترط أن تكون هذه البيانات والمعلومات التي تم الحصول عليها سرية، فيستوي أن تكون كذلك أم لا، الأهم هو أن تكون هذه البيانات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني. وتتم عملية إرسال نظم التجسس الإلكتروني بعدة طرق ومن أشهرها البريد الإلكتروني، حيث يقوم المجني عليه بفتح المرفقات المرسلة ضمن رسالة غير معروفة المصدر، وهناك طرق أخرى لزرع أحصنة طروادة، وكذلك عن طريق إنزال بعض البرامج من أحد المواقع غير الموثوق بها (عبد الإله مُحَمَّد النوايسة، وممدوح حسن العدوان، 2019م، ص 467 وما بعدها). لذلك عاقب المنظم السعودي على الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني، بعقوبة السجن لمدة لا تزيد على عشر سنوات وبغرامة لا تزيد على

خمسة ملايين ريال، أو بإحدى هاتين العقوبتين، وذلك وفقًا لنص المادة السابعة من نظام مكافحة جرائم المعلوماتية.

3.3 المطلب الثالث: وسائل الإرهاب الإلكتروني:

تسعى التنظيمات الإرهابية إلى استخدام التكنولوجيا لنشر مبادئهم وتصوراتهم، والقيام بعدة أعمال تخريبية عبر شبكة الإنترنت للوصول إلى أهدافها المرجوة، وتتبع في ذلك وسائل متعددة في سبيل تحقيق أهدافها ومقاصدها الإرهابية في تسهيل الاتصال بين قيادات وأعضاء المنظمات الإرهابية، واستقطاب الإفراد واستدراجهم للانخراط في مثل هذه التنظيمات، وإن أكثر وسائل الإرهاب الإلكتروني شيوعًا يتمثل في استخدام هذه التنظيمات للبريد الإلكتروني من أجل نشر أهدافها وثقافاتها وتجنيد أعضائها، بالإضافة إلى إنشاء مواقع خاصة بهذه التنظيمات على شبكة الإنترنت لخدمة أهدافها وتحقيق أغراضها. لذلك سنتناول هذه الوسائل من خلال الفروع التالية:

1.3.3 الفرع الأول: تبادل المعلومات والبيانات الإرهابية عبر الشبكة العنكبوتية:

تستخدم التنظيمات الإرهابية الشبكة العنكبوتية للتواصل والتنسيق وتبادل المعلومات فيما بينهم، نظرًا لسهولة الاتصال الآمن وسرعة لإيصال الرسائل، وذلك عن طريق استخدام البريد الالكتروني أو المواقع الإلكترونية والمنتديات وغرف الحوار الإلكتروني، إذ يمكن أن يلتقي عدة أشخاص في أماكن متعددة وفي زمن معين ويتبادلون الحديث والاجتماع مع بعضهم عبر الشبكة المعلوماتية. وتقوم التنظيمات الإرهابية باستخدام الشبكة المعلوماتية في نشر بياناتها الإرهابية، وذلك عن طريق المواقع الإلكترونية، وقد ساعدت القنوات الفضائية التي تسارع في الحصول على مثل هذه البيانات الإرهابية، ومن ثم تقوم بنشرها عبر وسائل الإعلام في مضاعفة انتشار تلك البيانات ووصولها إلى مختلف شرائح المجتمع، وتأخذ هذه البيانات الصادرة من قبل التنظيمات الإرهابية أساليب التهديد والترويع لشن هجمات إرهابية معينة، أو تصدر معلنة عن تبني تنفيذ عمليات إرهابية محددة؛ وذلك من أجل نشر الخوف والرعب بين الأفراد والدول في محاولة الضغط عليهم للرضوخ لأهداف تلك التنظيمات الإرهابية (أسامة جابر دوح، 2016م. ص 72 وما بعدها).

2.3.3 الفرع الثاني: إنشاء المواقع الإرهابية الإلكترونية:

يقوم الإرهابيون بإنشاء وتصميم مواقع لهم على الشبكة المعلوماتية لبث أفكارهم ودعوتهم، وتجنيد إرهابيين جدد، ولإعطاء التعليمات، ولشرح طرق اختراق البريد الإلكتروني، واختراق وتدمير المواقع الإلكترونية، والدخول إلى المواقع المحجوبة، ولتعليم طرق نشر الفيروسات، والتدريب الإلكتروني من خلال تعليم الطرق والوسائل التي تساعد على القيام بشن هجمات إرهابية، فقد أنشأت مواقع إرهابية إلكترونية تستخدم كمعسكرات تدريب افتراضي سري لنشر تعليمات تخص كيفية صناعة المتفجرات، وطرق تجهيز العبوات الناسفة، والتدريب على استخدامها من خلال كتيبات إلكترونية أو من خلال أشرطة فيديو تنشرعبر مواقعها الخاصة. وكما قامت بعض التنظيمات الإرهابية بإنتاج أدلة إرشادية للعمليات الإرهابية، وهذه الأدلة يمكن نشرها عبر الشبكة المعلوماتية لتصل إلى الإرهابيين في مختلف أنحاء العالم (محمود صالح العادلي، 2005م، ص 183).

3.3.3 الفرع الثالث: تدمير المواقع الإلكترونية والنظم المعلوماتية:

وتقوم التنظيمات الإرهابية بشن هجمات إرهابية إلكترونية من خلال الشبكة المعلوماتية؛ بقصد تدمير المواقع والبيانات الإلكترونية والنظم المعلوماتية، وإلحاق الضرر بالبنية المعلوماتية التحتية وتدميرها. مثال ذلك: هجوم إلكتروني على أحد المواقع الإلكترونية بقصد تدميرها وشلها عن العمل، حيث يمكن أن يقوم الإرهابيون بشن هجوم مدمر لإغلاق المواقع الحيوية على الشبكة المعلوماتية، وإلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات في الدول (حمزة محمد أبو عيسى، 2019م، ص 190).

4. المبحث الثالث: موقف التشريعات والاتفاقيات العربية من مواجهة الإرهاب الإلكتروني:

لقد ساعد التطور العلمي والتكنولوجي إلى ازدياد العمليات الإرهابية، وتفاقمت ظاهرة الإرهاب الإلكتروني، حيث تسخر الجماعات الإرهابية التكنولوجيا الحديثة بما لديها من أدوات في تنفيذ مخططاتها الإرهابية، وتحولت شبكة الإنترنت إلى أداة فعالة في تسهيل الاتصال بين قيادات المنظمات الإرهابية وأعضائها، وتجنيد الإرهابيين واستقطاب الشباب من خلال مواقع التواصل الاجتماعي، وتوجيه رسائل للإعلام بهدف تروع المجتمعات كأسلوب ضغط لتحقيق مطامعها السياسية، كعرض أفلام مرعبة للمختطفين أثناء إعدامهم، أو حرقهم أو قطع رؤوسهم. لذلك فرصت الدول العربية عقوبات لمكافحة جرائم الإرهاب الإلكتروني في قوانينها. لذلك سينقسم هذا المبحث إلى المطلبين التاليتين: المطلب الأول

موقف التشريعات العربية من مواجهة الإرهاب الإلكتروني، والمطلب الثاني موقف الاتفاقيات العربية من مواجهة الإرهاب الإلكتروني.

1.4 المطلب الأول: موقف التشريعات العربية من مواجهة الإرهاب الإلكتروني:

يعتمد الإرهاب الإلكتروني على استخدام الإمكانيات العلمية والتقنية، واستغلال وسائل الاتصالات والشبكات المعلوماتية، من قبل المنظمات الإرهابية لتنظيم وتنسيق عملياتهم المتفرقة والمنتشرة حول العالم، من أجل تخويف وترويع الآخرين، وإلحاق الضرر بهم، أو تهديدهم، والتجسس على الدول، لذلك كان لابد من إصدار تشريعات وقوانين رادعة للتصدي لظاهرة الإرهاب الإلكتروني ومكافحتها. لذلك سينقسم هذا المطلب إلى الفروع التالية: الفرع الأول موقف المنظم السعودي، والفرع الثاني موقف التشريع المصري، والفرع الثالث موقف التشريع الإماراتي، والفرع الرابع موقف تشريع إقليم كوردستان – العراق.

1.1.4 الفرع الأول: موقف المنظم السعودي:

في إطار الجهود الوطنية لمكافحة الإرهاب أصدرت المملكة السعودية العربية نظامًا قانونيًا خاصًا لمكافحة جرائم تقنية المعلومات، حيث وافق مجلس الوزراء على نظام مكافحة جرائم المعلوماتية بموجب المرسوم الملكي رقم (17) لعام 1428هـ. وتضمن هذا النظام صورًا للجرائم المعلوماتية بوجه عام، وجرائم الإرهاب الإلكتروني بشكل خاص. حيث جرم المنظم السعودي إنشاء مواقع إلكترونية لمنظمات إرهابية على الشبكة المعلوماتية، لتسهيل الاتصال بين قياداتها وأعضائها، أو لبث الأفكار والمواد المعادية للدين الإسلامي، أو تمويلها، وإرسال الأوامر والتعليمات للمتعاونين معهم حول كيفية صنع القنابل والمتفجرات واستعمالها في عملياتهم الإرهابية. فالعديد من التنظيمات الإرهابية المسلحة تعلن عبر شبكة الإنترنت عن حاجتهم لتجنيد عناصر تساعدهم في تنفيذ أعمالهم الإجرامية، وعملياتهم الانتحارية مستخدمة في ذلك الجانب الديني، كما جرم المنظم السعودي الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني، وهو يعد من أخطر أنواع الجرائم المعلوماتية.

لذلك يعاقب المنظم السعودي بعقوبة السجن لمدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين، على إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره؛ لتسهيل الاتصال بقيادات تلك المنظمات، أو أي من أعضائها، أو ترويج أفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات، أو أي أداة تستخدم في الأعمال الإرهابية. والدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني. وذلك وفقًا لنص المادة السابعة من نظام مكافحة جرائم المعلوماتية.

وحدد المنظم السعودي في نص المادة التاسعة من نظام مكافحة جرائم المعلوماتية على وسائل الاشتراك في الجريمة وهي ذاتها وسائل الاشتراك في أي جريمة أخرى، فسلوك الشريك يتمثل في الاتفاق على الجريمة، أو تحريضه على ارتكابها، أو مساعدة فاعلها لتمكينه من ارتكابها. ويعاقب المنظم على الاشتراك في جرائم الإرهاب الالكتروني بما لا يتجاوز الحد الأعلى للعقوبة المقررة لها، ويعاقب بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة لها إذا لم تقع الجريمة الأصلية. مثال على ذلك: تجهيز المكان المتواجد به حماز الحاسوب الذي سيتم الدخول من خلاله إلى المواقع الإلكترونية، أو الشبكة المعلوماتية، لإرسال رسائل بين أعضاء المنظمة الإرهابية، أو نشر والترويج لأفكارهم، أو التدريب على تصنيع المتفجرات، أو استغلال الشبكة المعلوماتية في تمويل الإرهاب، أو التجسس على الدول. ولابد إن يعلم الشريك بنشاط الفاعل الذي قام بإنشاء الموقع الإلكتروني، وبغاية الفاعل من هذا النشاط وهو تسهيل الاتصال بقيادات المنظمات الإرهابية، أو أعضائها، أو في نشر وترويج أفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرات، أو أي مادة تستخدم في الأعمال الإرهابية.

وجدير بالذكر أنه، ساوى المنظم السعودي في العقوبة بين الفاعل الأصلي والشريك في ارتكاب جرائم الإرهاب الإلكتروني، فيعاقب الشريك بما لا يتجاوز الحد الأعلى للعقوبة المقررة لها، ويتحقق الاشتراك في الجريمة غير التامة في الاشتراك في جريمة لم تقع أي توقفت عند مرحلة الشروع، فيعاقب الشريك بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة لها إذا لم تقع الجريمة الأصلية. وأبقى المنظم السعودي على العقوبة في حدها الأقصى عشر سنوات، غير أنه قيد القاضي بألا تقل عقوبة السجن أو الغرامة عن نصف حدها الأعلى، بمعنى إذا قررت المحكمة الحكم بعقوبة السجن فيجب ألا تقل العقوبة عن خمس سنوات، وإذا قضى بالغرامة فيجب ألا يقل مقدارها عن مليونين ونصف ريال.

وكما نصت المادة الثامنة من هذا النظام على أسباب تشديد العقاب المقرر للجريمة، حيث تنص على أنه "لا تقل عقوبة السجن أو الغرامة عن نصف حدها

الأعلى إذا اقترنت أي جريمة منها بظروف من الظروف المشددة للعقاب، وهي إذا ارتكاب الجاني الجريمة من خلال عصابة منظمة، أو الصفة العمومية للجاني، أو بالتغرير بالقصر واستغلالهم، أو بتحقق حالة العود إلى الجريمة". (النظام السعودي مكافحة جرائم المعلوماتية بموجب المرسوم الملكي رقم (17) لعام 1428هـ).

2.1.4 الفرع الثاني: موقف التشريع المصري:

تناول المشرع المصري جرائم الإرهاب الإلكتروني والترويج للتنظيمات الإرهابية وتمويلها في قانون مكافحة الإرهاب رقم (94) لسنة 2015م، وذلك في المادة (29) والتي نصت على أنه: "يعاقب بالسجن المشدد مدة لا تقل عن خمس سنين كل من أنشأ أو استخدم موقعا على شبكات الاتصالات أو شبكة المعلومات الدولية أو غيرها بغرض الترويج للأفكار، أو المعتقدات الداعية إلى ارتكاب أعمال إرهابية، أو لبث ما يهدف إلى تضليل السلطات الأمنية أو التأثير على سير العدالة في شأن أي جريمة إرهابية أو لتبادل الرسائل وإصدار التكليفات بين الجماعات الإرهابية أو المنتمين إليها، أو المعلومات المتعلقة بأعمال أو تحركات الإرهابيين أو الجماعات الإرهابية في الداخل والخارج". كما شدد المشرع المصري العقوبة في الفقرة الثانية من هذه المادة في حالة الدخول غير المشروع إلى موقع إلكتروني حكومي، للحصول على بيانات أو معلومات موجودة عليه أو الاطلاع عليها أو تغييرها أو محوها أو إتلافها أو تزوير محتواها، وذلك بغرض الترويج للأفكار، أو المعتقدات الداعية إلى ارتكاب أعمال إرهابية، أو لبث ما يهدف إلى تضليل السلطات الأمنية أو التأثير على سير العدالة في شأن أي جريمة إرهابية، أو لتبادل الرسائل وإصدار التكليفات بين الجماعات الإرهابية أو المنتمين إليها أو المعلومات المتعلقة بأعمال أو تحركات الإرهابيين أو الجماعات الإرهابية في الداخل والخارج. حيث نصت الفقرة الثانية على أنه: "يُعاقب بالسجن المشدد مدة لا تقل عن عشر سنين، كل من دخل بغير حق أو بطريقة غير مشروعة موقعاً إلكترونياً تابعاً لأية جهة حكومية، بقصد الحصول على البيانات أو المعلومات الموجودة عليها أو الاطلاع عليها أو تغييرها، أو محوها أو إتلافها أو تزوير محتواها الموجود بها، وذلك كله بغرض ارتكاب جريمة من الجرائم المشار إليها بالفقرة الأولى من هذه المادة أو الإعداد لها". كما نص المشرع المصري على جريمة تمويل الإرهاب في المادة (13) بقانون رقم (94) لسنة 2015م، والمعدل بقانون رقم 15 لسنة 2020م، في مادته الأولي والتي نصت على أنه:" يعاقب بالسجن المؤبد كل من ارتكب جريمة من جرائم تمويل الإرهاب إذا كان التمويل الإرهابي، وتكون العقوبة الإعدام إذا كان التمويل لجماعة إرهابية أو لعمل إرهابي أو إذا كان تمويل الإرهاب بقصد سفر أفراد إلى دولة غير دولة إقامتهم أو جنسيتهم بغرض ارتكاب عمل إرهابي أو التخطيط له أو إعداده أو المشاركة فيه أو تقديم العون أيا كان شكله. وفي الأحوال التي ترتكب فيها الجريمة بواسطة جماعة إرهابية أو شخص اعتباري، ويعاقب المسؤول عن الإدارة الفعلية لهذه الجماعة أو ذلك الشخص بالعقوبة الإعدام. وكما تعاقب الجماعة الإرهابية أو الشخص الاعتباري بغرامة لا تقل عن مائة ألف جنيه ولا تجاوز ثلاثة ملايين جنيه، وتكون مسئولة بالتضامن عن الوفاء بما يحكم به من عقوبات مالية أو تعويضات."

كما ساوى المشرع المصري في العقوبة بين الفاعل الأصلي والشريك في ارتكاب جرائم الإرهاب وذلك وفقاً لنص المادة (6) بقانون رقم (94) لسنة 2015م، والتي نصت على أنه:" يُعاقب على التحريض على ارتكاب أية جريمة إرهابية، بذات العقوبة المقررة للجريمة التامة، وذلك سواء كان هذا التحريض موجهاً لشخص محدد أو جماعة معينة، أو كان تحريضاً عاماً علنياً أو غير علني، وأياً كانت الوسيلة المستخدمة فيه، ولو لم يترتب على هذا التحريض أثر. كما يُعاقب بذات العقوبة المقررة للجريمة التامة كل من اتفق أو ساعد - بأية صورة - على ارتكاب الجرائم المشار إليها بالفقرة الأولى من هذه المادة، ولو لم تقع الجريمة بناءً على ذلك الاتفاق أو تلك المساعدة. كما نص المشرع المصري في المادة (7) من هذا القانون على أنه: "يُعاقب باعتباره شريكاً كل من سهل لإرهابي أو لجماعة إرهابية بأية وسيلة، مباشرة أو غير مباشرة ارتكاب أية جريمة إرهابية، أو الإعداد لارتكابها، أو وفر، مع علمه بذلك، لمرتكبها سكناً أو مأوى أو مكاناً للاختفاء، أو لاستخدامه في الاجتماعات أو غير ذلك من التسهيلات.(القانون المصري بشأن مكافحة الإرهاب رقم (94) لسنة 2015م، والمنشور بالجريدة الرسمية بالعدد 33 مكرر بتاريخ 15 أغسطس 2015م، والمعدل بقانون رقم 15 لسنة 2020م، والمنشور بالجريدة الرسمية بالعدد 9 مكرر أ بتاريخ 3 مارس 2020م).

3.1.4 الفرع الثالث: موقف التشريع الإماراتي:

صدر القانون الاتحادي رقم (2) لسنة 2006م بشأن مكافحة جرائم تقنية المعلومات، والمعدل بقانون 5 لسنة 2012م، حيث جرم المشرع الإماراتي الإرهاب الإلكتروني في قانون مكافحة جرائم تقنية المعلومات رقم (5) لسنة 2012م، حيث نصت المادة (26) على أنه: " يعاقب بالسجن مدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن مليون درهم ولا تجاوز مليوني درهم كل

من أنشأ أو أدار موقعا إلكترونيا أو أشرف عليه أو نشر معلومات على الشبكة المعلوماتية أو وسيلة تقنية معلومات، وذلك لجماعة إرهابية أو أي مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة بقصد تسهيل الاتصال بقياداتها أو أعضائها، أو استقطاب عضوية لها، أو ترويج أو تحبيذ أفكارها، أو تمويل أنشطتها، أو توفير المساعدة الفعلية لها، أو بقصد نشر أساليب تصنيع الأجهزة الحارقة أو المتفجرات، أو أي أدوات أخرى تستخدم في الأعمال الإرهابية".

كما ذكرت المادة (4) من هذا القانون على جريمة التجسس الإلكتروني، والتي نصت على أنه: "يعاقب بالسجن المؤقت والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون وخمسمائة ألف درهم كل من دخل بدون تصريح إلى موقع إلكتروني، أو نظام معلومات إلكتروني، أو شبكة معلوماتية، أو وسيلة تقنية معلومات، سواء كان الدخول، بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أو اقتصادية.

وقد اعتبر المشرع الإماراتي جرائم الإرهاب الإلكتروني من الجرائم الماسة بأمن الدولة، وذلك في المادة (44) من هذا القانون والتي نصت على أنه: "تعتبر الجرائم الواردة في المواد (4،24، 26،28، 29، 30،38) من هذا المرسوم بقانون من الجرائم الماسة بأمن الدولة. وكما تعتبر من الجرائم الماسة بأمن الدولة، أي جريمة منصوص عليها في هذا المرسوم بقانون إذا ارتكبت لحساب أو لمصلحة دولة أجنبية أو أي جماعة إرهابية أو مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة". وكما شدد المشرع الإماراتي العقوبة في المادة (46) من هذا القانون، والتي نصت على أنه:"يعد ظرفاً مشدداً استخدام شبكة المعلومات أو الإنترنت أو أي نظام معلوماتي إلكتروني أو موقع إلكتروني أو وسيلة تقنية معلومات عند ارتكاب أي جريمة لم ينص عليها هذا المرسوم بقانون. كما يعد ظرفا مشددا ارتكاب أي جريمة منصوص عليها في هذا المرسوم بقانون لحساب، أو لمصلحة دولة أجنبية، أو أي جماعة إرهابية، أو مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة (قانون اتحادي رقم 5 لسنة 2012م بشأن مكافحة جرائم تقنية المعلومات، والمنشور بالجريد الرسمية ب العدد 540 ملحق السنة (42) بتاريخ 26 أغسطس 2012م).

4.1.4 الفرع الرابع: موقف تشريع إقليم كوردستان - العراق:

جرم المشرع الكوردستاني جريمة الإرهاب في قانون مكافحة الإرهاب الصادر برقم 3 لسنة 2006م، حيث نصت المادة (1) من هذا القانون على تعريف الفعل الإرهابي، ونصت المادة (2) على الأفعال التي تعد أفعالاً إرهابية، حيث نصت الفقرة الثالثة منها على أنه: "يعاقب بالإعدام كل من استخدام بدوافع إرهابية لمواد مفرقعة أو متفجرة أو حارقة أو سريعة الاشتعال أو أجهزة مصممة للتخريب والهدم عن طريق التفجير مباشرة أو بواسطة أجهزة التحكم عن بعد أو تفخيخ آليات أو أية وسيلة أخرى أو زرع العبوات الناسفة أو استخدام الأسلحة الحربية بأنواعها المختلفة أو استعمال أحزمة ناسفة أو رسائل ملغومة أو مواد أو غازات سامة أو جرثومية أو مشعة إذا أدى الفعل إلى موت إنسان أو أكثر. وجرمت المادة (3) من هذا القانون في فقرتها الرابعة على تعطيل وسائل الاتصالات وأنظمة الحاسوب أو اختراق شبكاتها أو التشويش عليها أو إدخال معلومات أو بيانات فيها بهدف تسهيل ارتكاب الجرائم الإرهابية، ونصت الفقرة الخامسة منها على تمويل جرائم الإرهاب حيث نصت على أنه: "يعاقب بالسجن المؤبد كل من يقوم بتقديم، أو جمع، أو نقل، أو تحويل الأموال بطريق مباشر أو غير مباشر داخل الاقليم أو خارجه بقصد استخدامها أو علمه باستخدامها في تمويل أية جريمة إرهابية". كما نصت في الفقرة الثامنة على صنع، أو استيراد أو حيازة متفجرات أو مفرقعات أو أجهزة مصممة للتخريب أو الهدم أو أية مادة تدخل في تركيبها وكذلك الأجهزة والآلات والأدوات التي تستخدم في صنعها وتفجيرها إذا كان ذلك بقصد استخدامها لارتكاب إحدى الجرائم الإرهابية.

كما جرم المشرع الكوردستاني الشروع في ارتكاب جرائم الإرهاب حيث نصت المادة (5) في فقرتها (أ – ب) من قانون مكافحة الإرهاب الصادر برقم 3 لسنة 2006م على أنه: "يعاقب بالسجن المؤبد كل من شرع في ارتكاب أحدى الجرائم المنصوص عليها في المادة (الثانية) من هذا القانون. ب- يعاقب بالسجن المؤقت كل من شرع في ارتكاب أحدى الجرائم المنصوص عليها في المادة (الثالثة) من هذا القانون.

وساوى المشرع الكوردستاني في العقوبة بين الفاعل الأصلي والشريك في ارتكاب جرائم الإرهاب وذلك وفقاً لنص المادة (10) من هذا القانون والتي نصت على أنه: "كل من ساهم بوصفه فاعلاً او شريكاً او محرضاً في ارتكاب الجرائم الارهابية الواردة في هذا القانون يعاقب بالعقوبة المقررة لها". (قانون إقليم كوردستان - العراق بشأن مكافحة الإرهاب برقم 3 لسنة 2006م).

وقد نصت المادة (5) من قانون مكافحة الجرائم الإلكترونية العراقي لسنة 2019م، على جريمة التجسس الإلكتروني، حيث نصت الفقرة الثالثة منها على أنه: "يعاقب بالسجن مدة لا تقل عن سبع سنوات ولا تزيد على عشرة سنوات وبغرامة لا تقل عن (5000000) خمسة ملايين دينار عراقي ولا تزيد على (10000000) عشرة ملايين دينار عراقي كل من دخل عمداً موقعاً او نظاماً أو أجهزة حاسوب أو ما في حكمها، بقصد الحصول على بيانات او معلومات تمس الأمن القومي أو الاقتصاد الوطني للبلد أو قام بإلغاء بيانات أو معلومات تمس الأمن القومي للبلد أو الاقتصاد الوطني أو حذفها أو تدميرها أو تغييرها. كما شدد المشرع العراقي العقوبة في الفقرة الرابعة من هذه المادة حيث نصت على أنه: "تطبق العقوبة الاشد في حال كان مرتكب الجريمة موظفاً أو مكلفاً بخدمة عامة."

كما نصت (16) من هذا القانون على أنه: " يعد مرتكباً جريمة التحريض كل من حرض او ساعد او اتفق او اشترك مع الغير على ارتكاب جريمة من الجرائم المنصوص عليها في هذا القانون فأن لم تقع الجريمة عوقب بنصف العقوبة المقررة لها قانوناً، إذا وقعت الجريمة نتيجةً لذلك التحريض يعاقب المحرض بذات العقوبة المقررة لها (القانون العراقي بشأن مكافحة الجرائم الإلكترونية لسنة 2019م).

2.4 المطلب الثاني: موقف الاتفاقيات العربية من مواجهة الإرهاب الإلكتروني:

أصبح الإرهاب الإلكتروني من أخطر أنواع الإرهاب في العصر الحالي، نظرًا لاتساع نطاق استخدام التكنولوجيا الحديثة في العالم، ولذلك فقد عقدت العديد من الاتفاقيات والملتقيات والمؤتمرات والندوات حول ظاهرة الإرهاب الإلكتروني، ومن أبرزها على المستوى العربي، الملتقى العلمي الدولي والذي نظمه مركز الملك عبدالله بن عبد العزيز للدراسات الإسلامية المعاصرة بعنوان "الإرهاب الإلكتروني وطرق مكافحته" 2014م، وندوة "الإرهاب الإلكتروني ومخاطره والمواجهة الأمنية" والتي نظمتها أكاديمية الشرطة بوزارة الداخلية المصرية في27 ديسمبر 2015م، ومؤتمر جامعة الإمام مُحَمَّد بن سعود الإسلامية في 17 نوفمبر 2016م بعنوان "الإرهاب الإلكتروني وخططه ووسائل مكافحته"، والمؤتمر الدولي لتجريم الإرهاب الإلكتروني والذي عقد في أبوظبي خلال الفترة من 15 – 16 مايو 2017 بهدف صياغة منظومة من القوانين الدولية، للتصدي لجذور وامتدادات ظاهرة الإرهاب الإلكتروني، والذي شارك فيه نخبة من الخبراء في مجال القانون والجرائم الإلكترونية ومكافحة الإرهاب، من مختلف دول العالم. لذلك ستناول في هذا المطلب الاتفاقيات العربية من خلال الفروع التالية: الفرع الأول الاتفاقية العربية لمكافحة الإرهاب 1998م، والفرع الثاني اتفاقية دول مجلس التعاون لدول الخليج العربية لمكافحة الإرهاب 2004م، والفرع الثالث الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010م.

1.2.4 الفرع الأول: الاتفاقية العربية لمكافحة الإرهاب 1998م:

صدرت الاتفاقية العربية لمكافحة الإرهاب بعد اعتمادها من مجلسي وزراء الداخلية والعدل العرب في اجتماعها المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة بتاريخ 1998/4/22م، بهدف مكافحة الإرهاب وتمويله، وأودعت لدى الأمانة العامة للأمم المتحدة وأدرجت كوثيقة دولية، وصادقت عليها المملكة العربية السعودية في ٢٨-١-١٩٩٩م.

وتحتوي الاتفاقية العربية لمكافحة الإرهاب على 42 مادة، وتهدف هذه الاتفاقية إلى تعزيز التعاون فيما بينها لمكافحة الجرائم الإرهابية التي تهدد أمن الأمة العربية واستقرارها وتشكل خطر على مصالحها الحيوية. فنصت المادة الأولى في فقرتها الثانية على مفهوم الإرهاب: وهو كل فعل من أفعال العنف أو التهديد به أيا كانت بواعثه أو أغراضه، يقع تنفيذا لمشروع إجرامي فردي أو جماعي ويهدف إلى إلقاء الرعب بين الناس، أو ترويعهم بإيذائهم أو تعريض حياتهم أو حريتهم أو أمنهم للخطر، أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو تعريض أحد الموارد الوطنية للخطر.أما فقرتها الثالثة فنصت على مفهوم الجريمة الإرهابية: هي أي جريمة أو شروع فيها ترتكب تنفيذا لغرض إرهابي في أي من الدول المتعاقدة أو على رعاياها أو ممتلكاتها أو مصالحها يعاقب عليها قانونها الداخلي، كما تعد من الجرائم الإرهابية الجرائم المنصوص عليها في الاتفاقيات التالية، عدا ما استثنته منها تشريعات الدول المتعاقدة أو التي لم تصادق عليها. كما نصت المادة الثالثة من هذه الاتفاقية على مجموعة من التدابير الأمنية لمنع الجريمة الإرهابية حيث نصت على أنه: "تتعهد الدول المتعاقدة بعدم تنظيم، أو تمويل، أو ارتكاب الأعمال الإرهابية، أو الاشتراك فيها بأية صورة من الصور، والتزاما منها بمنع ومكافحة الجرائم الإرهابية طبقا للقوانين والإجراءات الداخلية لكل منها".

وتناولت الفصل الثاني منها على آليات التعاون في المجالات الأمنية والقضائية لمنع ومكافحة الجريمة الإرهابية، وأما الفصل الثالث فقد تم التعرض من خلاله إلى إجراءات الإنابة القضائي، أما الباب الرابع فتضمن أحكاماً ختامية. تاريخ الاطلاع

12/ 2/ 2023م، متاح على الموقع التالي: http://agoyemen.net/lib_details.php?id=204

2.2.4 الفرع الثاني: اتفاقية دول مجلس التعاون لدول الخليج العربية لمكافحة الإرهاب 2004م:

وقع وزراء الداخلية لدول مجلس التعاون الخليجي على اتفاقية أمنية لمكافحة الإرهاب، والمنعقدة بدولة الكويت بتاريخ 4مايو 2004م، وتحتوي اتفاقية مكافحة الإرهاب على 49 مادة، وتهدف هذه الاتفاقية إلى القضاء على الإرهاب بجميع أشكاله وأنشطته وسبل دعمه، والحيلولة دون بلوغ أي مصادر تمويل لأعضائه أو منظماته أو تقديم أية وسائل مساعدة لهم. والتعاون الأمني والقانوني بين الدول المتعاقدة. حيث نصت المادة الأولى في فقرتها الثانية على مفهوم الإرهاب كما سبق تعريفه في الاتفاقية العربية لمكافحة الإرهاب، وأما فقرتها الثالثة نصت على مفهوم الجريمة الإرهابية: هي أي جريمة أو شروع فيها ترتكب تنفيذاً لغرض إرهابي في أي دولة متعاقدة أو على ممتلكاتها أو مصالحها أو على رعاياها أو ممتلكاتهم يعاقب عليها قانونها الداخلي، وكذلك التحريض على الجرائم الإرهابية أو الترويج لها أو تحبيذها، وطبع أو نشر أو حيازة محررات أو مطبوعات أو تسجيلات، أياً كان نوعها، إذا كانت معدة للتوزيع أو لاطلاع الغير عليها، وكانت تتضمن ترويجاً أو تحبيذاً لتلك الجرائم.

كما نصت الفقرة الرابعة من المادة الأولى على أنشطة دعم وتمويل الإرهاب، وهو: كل فعل يتضمن جمع أو تسلم أو تسليم أو تخصيص أو نقل أو تحويل أموال أو عائداتها لأي نشاط إرهابي فردي أو جماعي في الداخل أو في الخارج، أو القيام لمصلحة هذا النشاط أو عناصره بأي عمليات صكية أو مصرفية أو تجارية، أو التحصل مباشرة أو بالواسطة على أموال لاستغلالها لمصلحته، أو الدعوة والترويج لمبادئه أو تدبير أماكن للتدريب أو الإيواء لعناصره، أو تزويدهم بأية أنواع من الأسلحة أو المستندات المزورة، أو تقديم أية وسيلة مساعدة أخرى من وسائل الدعم والتمويل، مع العلم بذلك. كما نصت المادة الرابعة من هذه الاتفاقية على "تعهد الدول المتعاقدة بأن تتعاون فيما بينها، بتقديم الدعم والمساندة الأمنية اللازمة لأي دولة منها تتعرض لخطر أو جرائم الإرهاب، وآثاره، وذلك وفقاً لمتطلبات وظروف كل دولة".

كما نصت المادة الثامنة عشرة من هذه الاتفاقية على "تتخذ كل دولة من الدول المتعاقدة التدابير المناسبة، وفقاً لتشريعاتها وأنظمتها الوطنية، لتحديد أو كشف أو تجميد أو حجز أي أموال مستخدمة أو مخصصة لغرض من أغراض أنشطة دعم وتمويل الإرهاب وعائداتها لمصادرتها أو تبادلها أو اقتسامها مع الدول المتعاقدة الأخرى إذا كانت تتعلق بنشاط إرهابي امتد على إقليمها أو أضر بمصالحها وكانت مصلحة الكشف عن هذا النشاط تقتضي ذلك".

كما نصت المادة الثالثة والأربعون على إدراج الجرائم الإرهابية المشار إليها بهذه الاتفاقية في القوانين والتشريعات المحلية بوصفها جرائم خطيرة، وأن تقرر لها العقوبات المناسبة التي تعكس جسامة تلك الجرائم الإرهابية (تاريخ الاطلاع 22/ 1/ 2023م، متاح على الموقع التالي:

https://almeezan.qa/AgreementsPage.aspx?id=1231&language=ar

3.2.4 الفرع الثالث: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010م:

وافق مجلسا وزراء الداخلية والعدل العرب في اجتماعهما المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بتاريخ 15/ 1432/1هـ-2010/12/21م، وصادقت المملكة العربية السعودية على هذه الاتفاقية بتاريخ4مارس2012م، وتأتي أهمية هذه الاتفاقية في ظل تزايد الاختراعات التقنية في الهواتف الذكية وأجهزة الحاسوب التي يختفي وراءها مجرموا الاختراقات للمواقع الإلكترونية وارتكاب الجرائم من خلال تقنية الحاسوب، ومنها جرائم الإرهاب الإلكتروني.

وتحتوي اتفاقية مكافحة جرائم تقنية المعلومات على 43 مادة، وتهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات لدرء أخطار هذه الجرائم، حفاظًا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها"، ونصت المادة الثانية من هذه الاتفاقية على مجموعة من التعريفات الهامة ومنها تعريف تقنية المعلومات، والنظام المعلوماتي، والشبكة المعلوماتية، ونجد في الفصل الثاني تفصيلًا للأفعال التي تعد مجرمة، حيث نصت المادة السادسة على جرائم التجسس الإلكتروني من خلال تجريم الدخول غير المشروع للحصول على معلومات حكومية سرية. كما جاءت المادة الخامسة عشرة من هذه الاتفاقية بذكر الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات والتي نصت على أنه "نشر أفكار ومبادئ جماعات إرهابية والدعوة لها، تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية، نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية، نشر

النعرات والفتن والاعتداء على الأديان والمعتقدات ". أما الفصل الثالث منها فقد تم التعرض من خلاله إلى نطاق تطبيق الأحكام الإجرائية، وفي الفصل الرابع تناول التعاون القانوني والقضائي، أما الفصل الخامس فتضمن أحكاما ختامية. تاريخ الاطلاع 14/ 2/ 2023م، متاح على الموقع التالي: www.arablegalnet.org

5. الخاتمة

استهدفت الدراسة التعرف على بيان دور الذكاء الاصطناعي في مواجهة جرائم الإرهاب الإلكتروني، فتعد الخوارزميات هي أساس الذكاء الاصطناعي، وأهم أركانه، وتكون مُعدّة سلفًا لتحليل كم هائل من المعلومات، وتقوم الخوارزميات بتحليل البيانات للمجرمين أو المتهمين، لتعطي نتائج مُستقبلية دقيقة بتنبؤ إمكانية وقوع جريمة إرهابية في المستقبل من عدمه.

فتستغل الجماعات الإرهابية الشبكة العنكبوتية لترويج لأفكارها في تجنيد الشباب، فتقوم بتصميم مواقع إلكترونية جاذبة لإغرائهم واستقطابهم، وتعليم وتدريب الإرهابيين على كيفية صنع المتفجرات والقنابل، أو حرب نفسية ضد الجمهور المستهدف للسيطرة على الرأي العام، أو ترويع وخلق حالة من الذعر والفوضى. لذلك كان لابد من ضرورة وجود الأنظمة القانونية والتشريعات التي تساهم في حماية الدول من ظاهرة الإرهاب الإلكتروني.

1.5 النتائج

- يعد الذكاء الاصطناعي أحد نواتج التطور التكنولوجي في العصر الحالي، حيث أصبح متوغل في جميع مجالات وفروع الحياة.
- يعد الذكاء الاصطناعي سلاحًا ذو حدين، إيجابيًا في تتبع وتعقب الجرائم والمجرمين وسلبيًا في استخدام الإرهابيين لأنظمة الذكاء الاصطناعي في ارتكاب جرائمهم الإرهابية.
- يلعب الذكاء الاصطناعي دور في الحد من جرائم الإرهاب الإلكتروني.
- يعتمد الذكاء الاصطناعي على خوارزميات متعلقة بتحليل وجمع البيانات، وبالتالي ستصبح له القدرة على التفكير واتخاذ القرارات وتنفيذها ذاتياً.
- تساعد تطبيقات الذكاء الاصطناعي في الكشف عن جرائم الإرهاب الإلكتروني المتوقع حدوثها في المستقبل، وبمدة كافية لتمكن السلطة المختصة بمكافحة هذه الجرائم بمنعها قبل ارتكابها.
- لا تكفي النصوص القانونية الجنائية التقليدية وحدها لتنظيم استخدام تقنيات الذكاء الاصطناعي في كشف والتنبؤ بجرائم الإرهاب الإلكتروني.
- تقع جرائم الإرهاب الإلكتروني بواسطة استخدام إحدى وسائل تقنيات المعلومات، لهذا تمثل وسائل تقنية المعلومات ركناً مفترضاً في هذه الجرائم.
- تتعدد صور جرائم الإرهاب الإلكتروني ووسائله، ويكمن الخطر فيها في سهولة استخدام الجماعات الإرهابية لوسائل الاتصالات الإلكترونية في تسهيل الاتصال بين قياداتها وأعضائهم، أو التجنيد الأشخاص الجدد، أو نشر وترويج لأفكارهم ومبادئهم، والتنظيم للمخططات الإرهابية، أو التدريب على تصنيع المتفجرات، أو استغلال الشبكة المعلوماتية في تمويل الإرهاب.
- تستخدم التنظيمات الإرهابية الشبكة العنكبوتية للتواصل والتنسيق وتبادل المعلومات فيما بينهم، وذلك عن طريق استخدام البريد الالكتروني أو المواقع الإلكترونية والمنتديات وغرف الحوار الإلكتروني، إذ يمكن أن يلتقي عدة أشخاص في أماكن متعددة وفي زمن معين ويتبادلون الحديث والاجتماع مع بعضهم عبر الشبكة المعلوماتية.
- نص المنظم السعودي والمشرع الإماراتي على جرائم الإرهاب الإلكتروني في قانون مكافحة جرائم تقنية المعلومات.
- لم ينص المشرع المصري على جرائم الإرهاب الإلكتروني في قانون مكافحة جرائم تقنية المعلومات.

2.5 التوصيات

بناءً على نتائج الدراسة السابقة، توصي الدراسة بما يلي:

- يجب إفراد نصوص خاصة بالذكاء الاصطناعي في قانون الإجراءات الجنائية تنص على إمكانية استخدام أنظمة الذكاء الاصطناعي في إجراءات الاستدلال والتحقيق الجنائي.
- لابد على المنظم السعودي النص على وسائل تقنية المعلومات ضمن التعريفات الأساسية لنظام مكافحة جرائم المعلوماتية بموجب المرسوم الملكي رقم (17) لعام 1428هـ.
- يتعين على المشرع المصري النص على جرائم الإرهاب الإلكتروني في قانون مكافحة جرائم تقنية المعلومات.

- ضرورة التعاون الدولي لإبرام الاتفاقيات الدولية الخاصة بمكافحة جرائم الإرهاب الإلكتروني وفرض القوانين والعقوبات على المجرمين.
- إنشاء محكمة دولية للأمن الإلكتروني للتعاون القضائي الجنائي الدولي، والإبلاغ عن قضايا الإرهاب الإلكتروني، لإنفاذ القواعد الدولية الإلكترونية للإرهاب على الدول والمنظمات الإرهابية والأفراد.
- ضرورة إنشاء منظمة عربية للتنسيق وتبادل خبرات التقنية والتكنولوجيا من أجل مكافحة ظاهرة الإرهاب عبر الشبكات المعلوماتية والأنظمة الإلكترونية.
- ضرورة حجب المواقع الإلكترونية المشبوهة التي تسعى إلى نشر الإرهاب والأفكار المتطرفة.
- ضرورة توعية أفراد المجتمع ومستخدمي شبكات الإنترنت بمخاطر الإرهاب الالكتروني وصورها وأساليب مواجهتها.
- تفعيل الدور الوقائي للمؤسسات التوعوية كالأسرة، والمدرسة، والجامعة، وأجهزة الأعلام، ومواقع التواصل الاجتماعي، وذلك بالتوعية بخطورة الإرهاب الإلكتروني على الأفراد والمجتمع والدولة، والسعي إلى تقوية الوازع الديني.

6. المراجع

1.6 المراجع العربية

1.1.6 الكتب

1. حمزة محمد أبو عيسى، جرائم تقنية المعلومات، دراسة مقارنة في التشريعات العربية، ط2، دار وائل للنشر والتوزيع، عمان، 2019م، ص 190.
2. خالد حسن لطفي، الإرهاب الإلكتروني، آفة العصر الحديث والآليات القانونية للمواجهة، ط1، دار الفكر الجامعي، الإسكندرية، 2018.
3. زين العابدين عواد كاظم الكردي، جرائم الإرهاب المعلوماتي - دراسة مقارنة، ط1، منشورات الحلبي الحقوقية، بيروت 2018م.
4. عامر مرعي حسن الربيعي، جرائم الإرهاب في القانون الجنائي - دراسة مقارنة، دار الكتب القانونية ودار شتات للنشر والبرمجيات، مصر، 2010 م.
5. عبد الله موسي، وأحمد حبيب، الذكاء الاصطناعي، ثورة في تقنيات العصر، المجموعة العربية للتدريب والنشر، الطبعة الأولى، 2019م.
6. عبير محمد أسعد، الذكاء الاصطناعي، دار البداية، الطبعة الأولى، 2017م
7. محمد علي سويلم، جرائم الإرهاب والإرهاب الإلكتروني - دراسة مقارنة، ط 1، المصرية للنشر والتوزيع، القاهرة 2018م.
8. محمود صالح العادلي، موسوعة القانون الجنائي للإرهاب، دار الفكر الجامعي، الاسكندرية، 2005م.

2.1.6 الرسائل العلمية

1. أسامة جابر دوح، جريمة الإرهاب الإلكتروني في التشريع الأردني، رسالة ماجستير، جامعة جرش، 2016م.
2. باسل فايز حمد، المواجهة التشريعية لجرائم الإرهاب الإلكتروني، رسالة ماجستير، جامعة العلوم الإسلامية العالمية، كلية الدراسات العليا، 2019م.
3. بدره هويمل الزين، الارهاب في الفضاء الالكتروني، دراسة مقارنة، رسالة دكتوراه، جامعة عمان العربية، 2012م.
4. عبدالله سعد محمدي، المسؤولية الجزائية عن التمويل الإلكتروني للجماعات الإرهابية، رسالة ماجستير، جامعة الإسراء، 2018م.
5. عمرو سيد البحيري، أثر تطبيقات الذكاء الاصطناعي على رفع كفاءة الأداء الأمني بالتطبيق على تأمين الطرق، رسالة دكتوراه كلية الدراسات العليا، أكاديمية الشرطة، 2019م.
6. مصطفى سعد مخلف، جريمة الإرهاب عبر الوسائل الإلكترونية، دراسة مقارنة بين التشريعين الأردني والعراقي، رسالة ماجستير، جامعة الشرق الأوسط، 2017م.

3.1.6 الأبحاث العلمية

1. إيمان بن سالم، جريمة التجنيد الإلكتروني للإرهاب وفقا لقانون العقوبات الجزائري، ط1، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين - المانيا، 2018م.
2. خالد حامد مصطفي، جرائم الإرهاب في نظام مكافحة جرائم المعلوماتية بالمرسوم الملكي رقم 17 بتاريخ 8/ 3/ 1428هـ، مجلة البحوث الأمنية، كلية الملك فهد الأمنية، 2016م، المجلد 25، والعدد 65، ص 93- 159.
3. عبد الإله محمد النوايسة، وممدوح حسن العدوان، جرائم التجسس الإلكتروني في التشريع الأردني، دراسة تحليلية، مجلة دراسات علوم الشريعة والقانون، 2019م، المجلد 46، العدد 1: ملحق 1، ص 460- 495.
4. علي أحمد إبراهيم، تطبيقات الذكاء الاصطناعي في مواجهة الجرائم الالكترونية، المجلة القانونية،2021م، المجلد 9، العدد 8، 2809 – 2836.
5. محمود سلامة الشريف، الطبيعة القانونية للتنبؤ بالجريمة بواسطة الذكاء الاصطناعي ومشروعيته، المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، 30 ديسمبر 2021م، المجلد3، العدد2، ص 341 – 359.
6. وجيه محمد سليمان، الذكاء الاصطناعي في التحري والتحقيق عن الجريمة، مجلة الميزان للدراسات الإسلامية، جامعة العلوم الإسلامية العالمية،2022م، المجلد 3، العدد 3، ص 449 – 478.

4.1.6 الاتفاقيات الدولية والقوانين

1. الاتفاقية العربية لمكافحة الإرهاب 1998م.
2. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010م
3. اتفاقية دول مجلس التعاون لدول الخليج العربية لمكافحة الإرهاب 2004م.
4. قانون اتحادي رقم 5 لسنة 2012م بشأن مكافحة جرائم تقنية المعلومات.
5. القانون المصري بشأن مكافحة الإرهاب رقم (94) لسنة 2015م والمعدل بقانون رقم 15 لسنة 2020م.
6. القانون المصري بشأن مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018م.
7. القانون العراقي بشأن مكافحة الجرائم الإلكترونية لسنة 2019م.

8. النظام السعودي مكافحة جرائم المعلوماتية، الصادر بموجب المرسوم الملكي رقم (17) لعام 1428هـ.
9. النظام السعودي بشأن مكافحة جرائم الإرهاب وتمويله، الصادر بموجب المرسوم الملكي رقم (21) لعام 1439هـ.
10. قانون إقليم كوردستان - العراق بشأن مكافحة الإرهاب برقم 3 لسنة 2006م.

2.6 المراجع الأجنبية

1. Brayne, S. (2017). Big data surveillance: The case of policing. American Sociological Review, 82(5), 977-1008.
2. Jean François casile, le code péal à lépreuve de la délinquance informatique, presse universitaires, D'AIX, Marseille, PUAM, 2002, P97.
3. John Knittel and Michael Soto, The Danger of Computer Hacking, The Rosen Publishing Group, ink, 2000.
4. Julien TAIEB, Prestataires techniques de l'internet le sens des responsabilités, 19 mai 2008, www.juriscom.net.
5. Mohamed bozabar,la criminalitéinformatiquesurl'internet, journal of law academic, N: 01, volume 26, faculté de droit, université du Koweit, 2002, P44.
6. Noose de Chris Paris, 2000, Techniques de blanchiment et moyens de lutte interdite, editeur ou du Centre français d'exploitation du droit de copie @Dunod http/www.Dunod.com.
7. Osoba, O. A., & Welser IV, W. (2017). An intelli- gence in our image: The risks of bias and errors in artificial intelligence. Rand Corporation. p. 4.
8. Parker, Fighting Computer Crime: A New Framework for Protecting Information, Butterworth Publishers, United States, 1998.
9. Scherer, Eric, Système mondial de documents reliés entre eux par des ordinateurs connectés en réseau et permettant de publier et de consulter via l Internet. Application bâtie sur l›Internet. La révolution numérique, glossaire. 2009, Editions Dalloz, collection A savoir.56.
10. Smith, G. J., & O'Malley, P. (2017). Driving pol- itics: Data-driven governance and resistance. The British Journal of Criminology, 57(2), 275-298.
11. -Virginie heem David G. hotte paris 2004, La lutte Centre Le blanchi- ment des capitaux, Librairie General de Droit et de Jurisprudence, EJA, Falguiere,57.
12. -Winograd, T. (2006). Thinking Machines: Can There Be? Are We? The Foundations of Artificial Intelligence. Derek Partridge & Yorick Wilks eds., p. 167.

3.6 المواقع الإلكترونية

1. الاتفاقية العربية لمكافحة الإرهاب 1998م، تاريخ الاطلاع 12/ 2/ 2023م، متاح على الموقع التالي: http://agoyemen.net/lib_details.php?id=204
2. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010م، تاريخ الاطلاع 14/ 2/ 2023م، متاح على الموقع التالي: www.arablegalnet.org
3. اتفاقية دول مجلس التعاون لدول الخليج العربية لمكافحة الإرهاب 2004م، تاريخ الاطلاع 22/ 1/ 2023م، متاح على الموقع التالي: https://almeezan.qa/AgreementsPage.aspx?id=1231&language=ar