# Electronic Terrorism is Legal Challenges and Illegal Practices

**Abdelrahman Ahmed Abdalla**
**University of Sharja**
**U21101435@sharjah.ac.ae**

**Halima Khalid Almidfa**
**University of Sharja**
**halmidfa@sharjah.ac.ae**

**Accepted Date: 6/2/2025.** **Publication Date: 1/4/2026.**



## Abstract

This study investigates the modern threat of cross-border electronic terrorism, which significantly impacts state security and is linked to various factors. It highlights the challenges in controlling and prosecuting electronic terrorism due to differing international criminal procedures for terrorist activities like inspection, investigation, and evidence collection. The study also finds that electronic terrorism, reliant on computers and the internet, differs significantly from traditional methods, making it harder to regulate and prosecute. This challenge is worsened by inadequate cybersecurity and inconsistent laws globally.

**Keywords**: Electronic Terrorism, Terrorist Organizations, Challenges, Electronic Prosecution, Sanctions.

# الإرهاب الإلكتروني التحديات القانونية والممارسات غير المشروعة

عبد الرحمن أحمد عبد الله *
جامعة الشارقة
U21101435@sharjah.ac.ae

حليمة خالد المدفع **
جامعة الشارقة
halmidfa@sharjah.ac.ae

تاريخ القبول: 2025/2/6. تاريخ النشر: 2026/4/1.

**المستخلص**

تناول هذا البحث الإرهاب الإلكتروني المعاصر والعابر للحدود الذي يُشكلُ خطورة على أمن الدولة ويُعدّ جريمة متداخلة العوامل السياسية والاقتصادية وغيرها، وبيّن البحث أنّ الإرهاب الإلكتروني من الجرائم الصعب ضبطها وملاحقتها بسبب اختلاف الإجراءات الجزائية المُتخذة بين الدول في متابعة النشاط الإرهابي كالتفتيش والتحقيق والمحاكمة والإثبات، وخلص البحث أنّ وسائل الإرهاب التقليدي تختلف عن الإرهاب الإلكتروني الذي يعتمد على الحاسب الآلي وشبكات الانترنت وتقنيات يَصعُب ضبطها وملاحقتها تقنياً أو قانونياً بسبب افتقار الدول لتحصين الفضاء الإلكتروني وعدم تناسق التشريعات بينها.

**الكلمات المفتاحية:** الإرهاب الإلكتروني، التنظيمات الإرهابية، التحديات، الملاحقة الإلكترونية، العقوبات.

* طالب ماجستير
** أستاذ مساعد دكتور

## المقدمة

## Introduction

إنّ ما يشهده العالم اليوم من تقدم في المعلوماتية ووسائل الاتصال وإتاحة التقنيات التكنولوجية أمام أي فرد وضرورة وجودها في التعاملات اليومية يعدّ ثورة غير مسبوقة في العالم، وما أصبحت عليه الحياة من متغيرات سريعة فرضت الاعتماد على وسائل الاتصال الحديثة والحواسيب الآلية والذكاء الصناعي في جميع مجالات الحياة لما تقدمه من منافع كتوفير الجهد والوقت في إنجاز المهام وسرعة ودقة في الأداء وأصبح الاستغناء عنها صعباً، ولا يمكن لمثل هذه التقنيات والوسائل الحديثة المتاحة لأي فرد أن تكون إيجابية بالمطلق بل باتت سلاحاً ذو حدين يهدد العالم بأكمله، فمن ناحية تُقدم تسهيلات في التعاملات اليومية ودقة في الأداء العملي ومن ناحية ثانية زادت أطماع العدو في استغلال هذه الوسائل لبثّ الذعر والكراهية والتحريض على العنف والقتل والتخطيط لعمليات خطرة غير مشروعة كالعمليات الإرهابية، وما أنتجته ثورة المعلوماتية اليوم من أساليب خطرة غير مشروعة يدعى بالإرهاب الإلكتروني، وقد انتشر استخدام هذا المصطلح في الآونة الأخيرة نتيجة كثرة العمليات الإرهابية الإلكترونية وظهور جرائم إرهابية إلكترونية متنوعة ناتجة عن التسهيلات التي أتاحتها المعلوماتية والأدوات التكنولوجية للمجموعات الإرهابية وساهمت في ابتكار طرق وأساليب إجرامية ذات مستوى عالٍ، واتخذ الإرهاب منحىً جديداً مختلفاً عن الإرهاب التقليدي بالإمكانيات التي يوفرها المجال الإلكتروني لارتكاب جرائم متعددة كالعنف والتحريض والتضليل وغيرها من الجرائم الجديدة التي لم يكن يشهدها العالم مسبقاً، ويعرّف الإرهاب الإلكتروني بأنه نوع من أنواع الإرهاب المعاصر والمعتمد بشكلٍ أساسي على استخدام تقنيات المعلومات وأجهزة الحاسب وشبكة الانترنت لأجل تحقيق أهداف سياسية أو تهديد الحكومات أو بثّ الذعر أو التخريب أو غيرها من الأشكال الإجرامية الإرهابية ذات الأثار السلبية[1]، ويبيّن هذا البحث قانون الإمارات العربية المتحدة القانون الاتحادي رقم 7 في شأن مكافحة الجرائم الإرهابية لسنة 2014م و المرسوم بقانون اتحادي رقم 34 في شأن مكافحة الشائعات والجرائم الإلكترونية لسنة 2021م[2]، وغيرها من القوانين التي تحدد كيفية التعامل مع ظاهرة الإرهاب الإلكتروني وتداعياتها بالتوازي مع تنبّه دول العالم إلى مخاطر هذه الظاهرة ووضع الدول قضية الإرهاب الإلكتروني في أولوياتها ومكافحتها ومحاربة مقترفيها ومحاكمتهم جزائياً والتصدّي للإرهاب الإلكتروني المستحدث الذي يُهدد الأمن والسلم الدولي.

**أهمية البحث:** تتجلّى أهمية هذا البحث كون أن الإرهاب أصبح يتخذ أشكالاً جديدة ويتطور مع تطور التكنولوجيا ومن ضرورة معرفة مفهوم الإرهاب الإلكتروني وأنواعه وأساليبه والمخاطر الناجمة عن هذا الإرهاب المرتبط بالوسائل والتقنيات الإلكترونية كما وتتجلّى الأهمية في ضرورة تسليط الضوء على تداعيات ممارسة هذا النوع من الإرهاب وتحدياته وتحليل الإطار القانوني المتعلّق بالإرهاب الإلكتروني والعقوبات المستحقة لمرتكبي جرائمه من خلال:

أ- إظهار التحديات التقنية والقانونية التي تحول دون القدرة على ملاحقة مرتكبي الجرائم الإرهابية الإلكترونية العابرة للحدود.

ب- تحليل كيفية مساهمة الأطر القانونية في بناء الأنظمة القوية والفعّالة القادرة على مواجهة مخاطر الإرهاب الإلكتروني والتصدّي لها.

ت- عرض لأهم التشريعات والقوانين التي نظمها المشرع الإماراتي لمكافحة الجرائم الإرهابية الإلكترونية ومقارنة هذه القوانين مع قوانين الدول الأخرى للاستفادة مما نصّته الأنظمة المقارنة في القضاء على أخطر أنواع الإرهاب المعاصر.

**مشكلة البحث:**

يعد الإرهاب الإلكتروني من أخطر التحديات القانونية التي تواجه الأنظمة القضائية في العالم، حيث تستخدم الجماعات الإرهابية وسائل تكنولوجية معقدة لتنفيذ هجماتها وعملياتها التخريبية، ومع توسع نطاق هذه العمليات ليشمل مجالات غير تقليدية، مثل استهداف البنى التحتية الحيوية واختراق الأنظمة الأمنية، أصبحت الأدوات القانونية التقليدية عاجزة عن ملاحقة هذه الجرائم بشكل فعال، ويطرح هذا البحث إشكالية أساسية تتمثل في مدى قدرة القوانين الجزائية الوطنية على التعامل مع الجرائم الإرهابية الإلكترونية، والتحديات التي تواجه الملاحقة الجنائية لهذه الجرائم من حيث جمع الأدلة وإثباتها، بالإضافة إلى العقوبات المطبقة على مرتكبيها.

**تساؤلات البحث:**

أ- ما هي التحديات التي تواجه الجهات القانونية في جمع الأدلة الرقمية المتعلقة بالإرهاب الإلكتروني؟

ب- كيف تؤثر حدود الدول على ملاحقة مرتكبي الجرائم الإرهابية الإلكترونية؟

ت- ما هي العقوبات المقررة في القوانين الوطنية على الجرائم الإرهابية الإلكترونية؟

ث- ما هي الوسائل القانونية المتاحة لتجاوز تحديات ملاحقة الجناة الذين يرتكبون هذه الجرائم عبر الحدود؟

**منهجية البحث:** نعتمد في هذا البحث بشكلٍ أساسي على **المنهج الوصفي التحليلي والمنهج المقارن:**

أ- **المنهج الوصفي التحليلي**: القائم بشكل أساسي على بيان مفهوم الإرهاب الإلكتروني وأساليب ارتكاب الجرائم الإرهابية الإلكترونية وتحليل كيفية ملاحقة مرتكبي هذه الجرائم ووصف التحديات التي تعترض إمكانية كشف تلك الجرائم الإرهابية والوقوف على أبرز التشريعات والقوانين الناظمة لهذا النوع من الجرائم.

ب- **المنهج المقارن**: معتمدين بشكلٍ رئيسي على القانون الإماراتي مقارنة مع القانون المصري وتوضيح مدى الاستفادة من تشريعات وتجارب الجمهوريّة المصريّة في تطوير التشريعات الإماراتية ذات الشأن ومعرفة الإجراءات القانونية والتنظيمية التي اتخذتها بحقّ الفاعلين لجرائم الإرهاب الإلكتروني.

**خطة البحث:**

بالإضافة إلى المقدمة السابقة فقد قمنا بتقسيم البحث إلى مبحثين على الشكل الآتي:

**المبحث الأول: التحديات الراهنة في مكافحة الإرهاب الإلكتروني**

المطلب الأول: التحديات التقنية

المطلب الثاني: التحديات القانونية

**المبحث الثاني: الجرائم الإلكترونية الإرهابية: الجزاءات من العقوبات**

المطلب الأول: أساليب ملاحقة مرتكبي الجرائم الإلكترونية الإرهابية

المطلب الثاني: العقوبات القانونية على مرتكبي الجرائم الإرهابية الإلكترونية

## المبحث الأول

## The First Topic

## التحديات الراهنة في مكافحة الإرهاب الإلكتروني

## Current Challenges in Combating Cyber Terrorism

ظاهرة الإرهاب الإلكتروني ازداد انتشارها اليوم مع تطور التقنيات المعلوماتية والتكنولوجية وبات الإرهابيون يعتمدون على الشبكات العالمية لتنفيذ مخططاتهم الإرهابية وتعدّ هذه الظاهرة المعاصرة عابرة للحدود بظلّ وجود وسائل الاتصال وشبكات الانترنت[3]، لسهولة اقتناء هذه الوسائل وتوظيفها في الأعمال الإرهابية في أي مكان حول العالم بوقت قياسي مقارنة بالوسائل التقليدية مما يُكسب قضية الإرهاب حُلّة جديدة وأساليبَ لم تكن معروفة مسبقاً، وهذه الحلّة الجديدة من الإرهاب لابدّ من مكافحتها لأنها تشكل انتهاكاً لحقوق الإنسان التي أكدت الأمم المتحدة على احترامها وحماية حقوق الإنسان ومكافحة الإرهاب غايتان متكاملتان[4]، والالتزامات الدولية الخاصة بحقوق الإنسان تعدّ جزءاً من الإطار القانوني التنظيمي الخاص بمكافحة الإرهاب الإلكتروني والحد من خطورته على الأمن والسلم الدولي، ولأنّ أغلب الدول حول العالم باتت تعتمد على أجهزة الحاسب والتقنيات التكنولوجية في تعاملاتها والبنية التحتية للدول تُدار عن طريق الانترنت[5]، فتكون أكثر عُرضة من أي وقت مضى للهجمات والاعتداءات من قبل الإرهابيين الإلكترونيين.

لذلك نظمّت الدول القوانين بشأن مكافحة الإرهاب الإلكتروني كالقانون الاتحادي رقم 7 لسنة 2014 الصادر عن رئيس دولة الإمارات العربية المتحدة في شأن مكافحة الجرائم الإرهابية[6]، والمرسوم بقانون اتحادي رقم 20 في دولة الإمارات العربية المتحدة في شأن مواجهة جرائم غسل الأموال ومكافحة تمويل الإرهاب وتمويل التنظيمات غير المشروعة لسنة 2018م[7]، والمرسوم بقانون اتحادي رقم 34 في دولة الإمارات العربية المتحدة في شأن مكافحة الشائعات والجرائم الإلكترونية لسنة 2021م[8]، وقانون مكافحة الإرهاب في جمهورية مصر العربية قرار رئيس جمهورية مصر العربية بالقانون رقم 94 لسنة 2015 بإصدار قانون مكافحة الإرهاب الموجود في الجريدة الرسمية العدد 33 أغسطس سنة 2015[9]، وازداد الاهتمام بجرائم الإرهاب الإلكتروني في الوقت المعاصر بسبب ازدياد الهجمات والاعتداءات الإلكترونية على البنية التحتية للدول والأنظمة الإدارية والعسكرية والاستخباراتية وغيرها مما تطلّب اتخاذ التدابير الإجرائية لمنع تفشي هذه الظاهرة والحدّ منها ومواجهتها في مراحلها الأولى، وقد نصّ القانون الاتحادي رقم 20 لسنة 2018 بدولة الإمارات العربية المتحدة في شأن مواجهة جرائم غسل الأموال ومكافحة تمويل الإرهاب وتمويل التنظيمات غير المشروعة في المادة 4 أنّ الشخص الاعتباري يكون هو المسؤول من الناحية الجزائية عن أي جريمة يرتكبها هو أو تُرتكب باسمه الشخصي من قبل فرد آخر أو من خلال حسابه الخاص بالإضافة إلى المسؤولية المترتبة على المقترف الحقيقي للجريمة[10]، وهذا النوع من جرائم الإرهاب لا يُكتشف بالوسائل التقليدية لأنّه لا يستخدم الأسلحة المادية ذات الآثار المباشرة لذلك لابدَّ من قيام الدول بوضع استراتيجية خاصة لكشف الإرهاب الإلكتروني وآثاره ورسم المعالم القانونية والجنائية المتعلّقة بمكافحته[11]، بما يُساهم في التصدّي لهذا الخطر العابر للحدود وتحدّياته، وبناءً عليه قسّمنا المبحث الأول إلى مطلبين نتحدّث في المطلب الأول عن التحديات التقنية التي تواجه إمكانية مكافحة الإرهاب الإلكتروني.

## المطلب الأول

## The First Requirement

### التحديات التقنية

### Technical Challenges

يتميّز الإرهاب الإلكتروني أنّه لا يتطلّب استخدام القوة أو الأسلحة وإنّما كُل ما يحتاجه الإرهابي هو وجود كمبيوتر أو جهاز متصل بالإنترنت أو الشبكة المعلوماتية ومزوّد بالتطبيقات والبرامج الإلكترونية، ويلجأ الإرهابيون إلى هذا الأسلوب الليّن للتحريض والتأثير في وجهات نظر وأفكار الرأي العام وزعزعة أمن الدولة نظراً لما يوفره المجال الرقمي من سرعة وصول المعلومات وانتشارها بمجال واسع[12]، ومن الجرائم التي تعدّ مزعزعة لأمن الدولة تلك المرتكبة لصالح دولة أجنبية أو مجموعة إرهابية أو

منظمة أو جمعية أو هيئة غير مشروعة وفقاً للمادة60 من القانون الاتحادي رقم 34 لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية لدولة الإمارات العربية المتحدة[13]، وإنّ أي شخص قادر على الولوج إلى مواقع التواصل الاجتماعي وإنشاء مواقع إلكترونية للقيام بأنشطة تخريبية وأعمال غير مشروعة وكذلك التنظيمات الإرهابية قادرة على الترويج لعملياتها وجذب الداعمين واستقطاب الأفراد لتحقيق المزيد من العمليات الإرهابية[14]، وتطورت هذه العمليات في السنوات الأخيرة بتطور تقنيات المعلومات وظهور الذكاء الاصطناعي الذي أصبح جزءاً من استراتيجيتها اللوجستية والإعلامية كما سنوضح في الفقرات الأتية:

**أ- استخدام التقنيات المعلوماتية والذكاء الصناعي: Use of Information Technologies and Artificial Intelligence**

يُتقِن الإرهابيون المهارات التكنولوجية والخبرة بمجال المعلوماتية لتحقيق أهدافهم بزيادة سعة نشاطاتهم وجذب وتجنيد أعضاء لتنفيذ مخططاتهم بأفضل النتائج وبناءً عليه ورد في المرسوم بقانون اتحادي رقم 34 لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية في الإمارات العربية المتحدة المادة 60 تحت عنوان الظروف المشدّدة أنّ استعمال الفاعل للمواقع الإلكترونية أو شبكات المعلومات أو أي نظام معلوماتي إلكتروني أو غيرها من الوسائل التقنية في ارتكاب جريمته يعدّ ظرفاً مشدّداً يؤخذ بعين الاعتبار[15]، لأنّ ما يميّز التقنيات المعلوماتية والتكنولوجية الحديثة ليس فقط تنوعها وسهولة اقتنائها من قبل أي فرد بل إنّه من الصّعب إبقاء هذه المقتنيات بعيدة عن يد الإرهابي ويستغل الإرهابيون أنّ المستهلكين والتجار يدفعون للحصول على هذه الشبكات المعلوماتية والتكنولوجية في جميع دول العالم[16]، والجرائم المرتكبة عن طريق الإنترنت يستخدم فيها الدليل الرقمي في الإثبات الجنائي وقد أكدت المادة 65 من المرسوم بقانون اتحادي رقم 34 لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية بدولة الإمارات العربية المتحدة أنّ الأدلة المستخلصة من المواقع الإلكترونية أو الأنظمة المعلوماتية أو البرامج الحاسوبية أو إحدى الوسائل التقنية تعدّ حجة مادية للأدلة الجنائية في الإثبات الجنائي[17]، والإرهابيون يُنشئون مواقع على الشبكة المعلوماتية ومحتويات رقمية لتعليم المجندين كيفية تنفيذ العمليات الإرهابية وتدمير المواقع الإلكترونية المستهدفة وطرق نشر الفيروسات وإتلاف الأنظمة الخبيرة وطرق صناعة المتفجرات والأسلحة الكيماوية ومواقع لجني الأموال وتمويل الإرهابيين[18]، وقد وضّح المشرّع الإماراتي معنى تمويل الإرهابيين وتمويل التنظيمات الغير مشروعة في المرسوم بقانون اتحادي رقم 20 لسنة 2018 في شأن مواجهة جرائم غسل الأموال ومكافحة تمويل الإرهاب وتمويل التنظيمات الغير مشروعة واقتصره على الفعل المادي أو تقديم الأموال أو تحصيلها أو تخزينها أو إدارتها أو التصرّف الذي يراد من خلاله تقديم المال[19].

بخلاف ما تضمّنه قرار رئيس جمهورية مصر العربية بالقانون رقم 94 لسنة 2015 بإصدار قانون مكافحة الإرهاب في المادة 3 حيث استخدم توضيحاً شاملاً لمعنى تمويل الإرهاب وهو توفير أو جني أو تلقي أو إمداد بالأموال أو الأسلحة أو ذخائر أو معلومات أو بيانات مباشرة أو غير مباشرة بوسيلة رقمية أو إلكترونية لارتكاب أعمال إرهابية[20]، ونجد أنّ تمويل الإرهاب كما ذكر المشرّع المصري لم يقتصر على المكاسب المادية والربحية كما عرّفه المشرّع الإماراتي بل شمل التمويل الرقمي والتمويل بالوسائل الإلكترونية أو توفير المعلومات والبيانات اللازمة للعمليات الإرهابية أي كل أشكال التمويل الربحي أو تمويل بالمعلومات أو بالوسائل اللازمة لإتمام العمليات الإرهابية. وفي السنوات الأخيرة تطوّرت أساليب الإرهابيين بتطور تقنيات الذكاء الاصطناعي وتطور تقنيات التعلّم الآلي والتعلّم العميق، هذه التقنيات التي تركز على محاكاة دماغ الإنسان عن طريق تطوير الشبكات العصبونية الاصطناعية ويستخدم الإرهابيون هذه التقنية لصناعة فيديوهات وإنتاج صور ومقاطع فيديو للترويج لأفكارهم التطرّفية وجذب مجندين وأعضاء للانضمام لصفوف الإرهابيين نتيجة إعجابهم بالمحتويات الإرهابية المُعدّة بالذكاء الاصطناعي[21].

ومما سبق نلاحظ أنّ جرائم الإرهاب الالكتروني تختلف عن الإرهاب التقليدي وإنّ ثورة التحول الرقمي تُخلق صعوبات من ناحية إثبات الجرم الجنائي فمن غير الممكن فحص مسرح الجريمة كما في جرائم الإرهاب التقليدي للبحث عن أدوات أو آثار للمجرمين لأنّ الجرائم التي ترتكب عن طريق الشبكات المعلوماتية قد لا يترتب عليها أيّة آثار مادية، وتتمّ بصورة هادئة لا يلاحظها أي شخص ومن الصعب وضع المجرم تحت المراقبة ومن الممكن ألّا يتم اكتشاف الجريمة الإرهابية إلّا بعد أن يتم تنفيذها[22]، عدا عن إمكانية دخول أعداد من المستخدمين للشبكة والتغيير أو العبث بمجريات الجريمة ومحو آثارها[23].

### ب- تدابير المراقبة والاحتراز: Surveillance and Precautionary Measures

بدأت دول العالم بمراقبة الشبكة المعلوماتية والمواقع الإلكترونية وفَرَضَت الرقابة على المحتويات التي يبثها الإعلام لمنع دخول الفكر الإرهابي لأذهان الأفراد أو هيئات الدولة، ومن هذه الدول الإمارات العربية المتحدة وفق ما ظهر في المرسوم بقانون اتحادي رقم 34 في شأن مكافحة الشائعات والجرائم الإلكترونية لسنة 2021م حيث فرض التزامات على مستخدمي شبكات المعلومات والتأكيد على عدم بثّ محتويات غير قانونية مما يعدّ بمثابة ترشيد مسبق من الحكومة حول استخدام الإنترنت والشبكات المعلوماتية للوقاية من مخاطر الإرهاب الإلكتروني والتصدّي للتحديات الإرهابية[24]، وفي جمهورية مصر العربية ظهر مؤخراً قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018م حيث فرض القانون التزامات على مقدمي الخدمات

عبر الشبكة وألزمهم بالتقيّد بالواجبات الأمنية والتقنية التي تحددها الجهات المختصة والتعاون مع السلطات القضائية في تقديم المعلومات المطلوبة[25]، وتعمل الحكومات على وضع سياسات واستراتيجيات خاصة بمكافحة الإرهاب الإلكتروني لإفشال مخططاتِه وعملياته وذلك بمشاركة جميع فئات الحكومة من تقنيين ومبرمجين ووسائل الإعلام والأجهزة الأمنية وأفراد المجتمع وغيرهم، ومن التدابير الاحترازية التي تعمل الدول على تحقيقها للتصدّي للإرهاب الإلكتروني هي نشر الوعي الثقافي لضرورة حماية البيانات الشخصية وخصوصيتها وقد عرّف قانون مكافحة الشائعات والجرائم الإلكترونية في الإمارات العربية المتحدة في المرسوم بقانون اتحادي رقم 34 لسنة 2021م البيانات والمعلومات الحكومية والبيانات والمعلومات الشخصيّة والبيانات والمعلومات السريّة[26]، وذلك بصدد التمييز بين حقوق الهيئات والمؤسسات والأفراد ومعلوماتهم ومراسلاتهم وممارساتهم عبر الشبكة.

عَمِلَت الدول أيضاً على التنسيق الإلكتروني مع محركات البحث لمنع استخدامها كأداة لبثّ الفكر الإرهابي كموقع جوجل ويوتيوب وفيس بوك وويندوز لايف وغيرها من المواقع والحرص على أخذ الحذر من أن تكون هذه المواقع داعمة أو حامية للإرهاب والأفكار الإرهابية[27]، وحثّت على تعزيز الاتفاقيات الدولية المشتركة للدعم الفني والتقني والمادي للحكومات والهيئات والوكالات وتبادل المعارف والخبرات والمعلومات اللازمة لمواجهة الإرهاب الإلكتروني وتأمين بيئة استراتيجية قادرة على مواجهة الأشكال المتجددة لتحديات الفضاء الإلكتروني وتنسيق قوانين منفصلة خاصة بالأمن الإلكتروني تتوافق مع القوانين الدولية[28]، كنموذج موحد ومعتمد دولياً وقد أثبتت التجارب الدولية أنّ مكافحة الإرهاب الإلكتروني لا زالت تواجه تحديات وصعوبات سنتحدث عنها في المطلب الثاني التحديات القانونية.

## المطلب الثاني

## The Second Requirement

## التحديات القانونية

## Legal Challenges

سيادة القانون وسمّوه واحترام حقوق الأفراد وحماية حرياتهم جزءٌ أساسيٌّ من المساعي الدولية في مكافحة الإرهاب واحترام المعايير الدولية للحقوق والحريات الإنسانية خلال مراحل المكافحة أمرُ ضروري بدءاً من المراحل الأولى المتعلّقة بجمع المعلومات والمعطيات الاستخباراتية، وانتهاءً بتطبيق القواعد القانونية المستحقة على مقترفي جرائم الإرهاب بأنواعه عموماً وجرائم الإرهاب الإلكتروني خصوصاً لكونه الأكثر خطورة وهذا يتطلّب استحداث قوانين وتشريعات على المستوى الدولي والوطني لمكافحة الإرهاب وحماية حقوق الإنسان وسيادة القانون[29]، وبالرغم من

عدم وجود محتوى قانوني موحد دولياً لمصطلح **"الإرهاب"** أو يصفه كلياً[30] إلا أنّ مدلول هذا المصطلح في تطور دائم منذ نشأته، والإرهاب الإلكتروني الذي بدأ في نهايات القرن الماضي كان أحدث أنواع الإرهاب ويتطور بطبيعة الأحوال بتطور التكنولوجيا مما جعل وضع تعريف محدد وواضح لهُ أمراً صعباً لأنّ التعريف بالإرهاب الإلكتروني يختلف من مكان لآخر ويتطور بتطور البيئة الافتراضية المتوفرة لاحتضان هذا النوع من الجرائم، وجرائم الإرهاب عموماً تحمل صفة سلبية تشمل التهديد والرعب والعدوان والحرب النفسية أو الدينية أو السياسية على الدول لذلك عمدت الأمم المتحدة إلى إنشاء لجنة خاصّة بدراسة أسباب العمليات الإرهابية ودوافعها وتداعياتها[31]، وبالرغم من محاولات معظم الدول تدارك المخاطر الإلكترونية من خلال النظم القانونية الموضوعة لاستخدام تقنيات المعلومات والانترنت كمصر والإمارات وسوريا وإيطاليا وأستراليا وغيرها من الدول، إلا أنّ مواجهة الجرائم الإرهابية الإلكترونية جنائياً لا زال يطغى عليها قصوراً بسبب عدم توافر نصوص قانونية كفيلة بمعالجة المشكلات المتطورة عبر الإنترنت[32]، وسعى القوانين الجنائية إلى مكافحة تحديات الإرهاب الإلكتروني بالوسائل التقليدية لا تفي بالغرض لأنّ وجود جرائم متطورة وجديدة إرهابية عبر الإنترنت العابر للحدود لا يمكن المعاقبة عليه من خلال قانون العقوبات الذي يستند أساساً على ارتباط المجرم بمكان خاص، وكان المشرع الإماراتي أول المتصدين للجرائم الإرهابية كما ورد في المرسوم بقانون اتحادي رقم 20 في دولة الإمارات العربية المتحدة في شأن مواجهة جرائم غسل الأموال ومكافحة تمويل الإرهاب وتمويل التنظيمات غير المشروعة لسنة 2018م[33]، وكذلك المشرّع المصري تصدّى للجرائم الواقعة عبر الوسائل الرقمية والإلكترونية كما ورد في القانون المصري رقم 94 لعام 2015م الصادر عن رئيس الجمهورية بشأن مكافحة الإرهاب[34].

ولكن التحولات التكنولوجية المتسارعة تفرض على الدول واقعاً جديداً وتحدياتٍ أمنية وقانونية تحول دون إمكانية حماية أمن الدولة وما صنعته الثورة المعلوماتية من ابتكارات في الأساليب والأدوات الجديدة التي غيّرت طبيعة الصراعات والنزاعات الحربية من حروب تقليدية عسكرية بأسلحة مادية إلى حروب سيبرانية وإرهابية إلكترونية حتماً الفائز بها هو الأجدر على استخدام هذه التقنيات والدول ذات المهارات الاستخباراتية الأقوى، ولعلّ إحدى الصعوبات التي تواجه كشف هذه الجرائم أيضاً من الناحية القانونية هو عدم تناسق التشريعات بين الدول بشأن الإرهاب الإلكتروني مما يجعل المجرمين بمنأى عن العدالة وغالباً ما يكون الفاعلين خارج نطاق الدولة مما يساهم في إفلاتهم من وجه العدالة[35]، ومواجهة هذا النوع من الإرهاب تتطلّب تكثيف الجهود الدولية والوطنية وتوحيد أفكار وآراء السياسيين والدبلوماسيين والعسكريين للوصول إلى نقطة مشتركة حول تعريف العمليات الإرهابية الإلكترونية ووضع

استراتيجية لمكافحتها، وكانت أول اتفاقية موقعة لمكافحة جرائم الانترنت هي اتفاقية بودابست التي صادق عليها حوالي 30 دولة عُقِدَت هذه الاتفاقية في عام 2001م بالعاصمة المجرية بودابست عُنيت هذه الاتفاقية بمكافحة جرائم الانترنت وجرائم الإرهاب الإلكتروني وتعدّ استكمالاً للتوصيات الصادرة عن المجلس الأوروبي عام 1995 المرتبطة بالإجراءات الجزائية اللازمة لجرائم تقنيات المعلومات، إلّا أنّ هذه الاتفاقية لم تكن كافية حيث أنها لم تذكر سوى الجرائم الأكثر شيوعاً في العالم ومن ضمنها جرائم الإرهاب الإلكتروني وتطرقت إلى الطرق المتّبعة في التحقيق من هذه الجرائم وأكدت على ضرورة بذل الجهد والمساعي الدولية لمكافحة الإرهاب الإلكتروني[36].

ومن ثمّ على المستوى الإقليمي كانت الاتفاقية الوحيدة التي تطرّقت لقضايا مكافحة الإرهاب الإلكتروني هي المعاهدة العربية الصادرة في عام 2010م لمكافحة جرائم تقنية المعلومات وورد فيها أشكال متعلّقة بالجرائم الإرهابية التي ترتكب عن طريق الوسائل التقنية كالتحريض على الفتن والنعرات الطائفية وبثّ الذّعر ونشر الأفكار والمبادئ الإرهابية المتطرّفة والدعوى لجذب الأعضاء وتدريبهم على استخدام تقنيات الاتصال وتعليم طرائق صناعة المتفجرات والمواد السّامة والسّعي للحصول على التمويل للعمليات الإرهابية[37]، كل هذه الجرائم تندرج تحت مسمى جرائم العمليات الإرهابية الإلكترونية لكونها تستخدم تقنيات المعلومات كوسيلة لممارسة أعمالها كما ورد في الاتفاقية لكن يوجد جانب هام لم تذكره الاتفاقية وهو الأحكام الجنائية التي تحدد المسؤولية المترتبة على هذه الأعمال الغير مشروعة أو أحكام قانونية جنائية تتناسب مع الدّول الأعضاء في الاتفاقية كما أنّه لم تُشِر الاتفاقية إلى آلية أو دعوة لإنشاء مركز أو هيئة إقليمية متخصّصة في مكافحة الجرائم الإرهابية الإلكترونية، وهذا ما يجعل الاتفاقية منقوصة الجوانب مما يحول دون التصدّي لعواقب وأضرار الإرهاب الإلكتروني وعلى الرغم من إدراك الدول لمخاطر الإرهاب الإلكتروني وسعيهم لضرورة وجود أحكام قانونية وأنظمة تضبط التعاملات الإلكترونية إلّا أنّ هذه الأنظمة والتشريعات ليست موحدة بين الدول وإلى اليوم لا يوجد نموذج موحد لتطبيق أحكام جزائية لمكافحة الإرهاب الإلكتروني[38]، بسبب الاختلاف بثقافات الشعوب وعاداتهم وتقاليدهم حول العالم وسعة النشاطات الإجرامية الإلكترونية وما يكون مباحاً في إحدى الدول قد يكون إجراماً في دولة أخرى[39]، وأيضاً اختلاف وتنوع الإجراءات الجزائية المُتخذة في متابعة النشاط الإرهابي كالتفتيش والتحقيق والمحاكمة وطرق جمع الدلائل والإثبات تختلف من دولة لأخرى[40].

ومن جانب آخر تنازع الاختصاص على المستوى الدولي لأنّ جرائم الإرهاب الإلكتروني هي جرائم عابرة للحدود فقد تُرتكب الجريمة بدولة معيّنة من قبل إرهابيين قاطنين في دولة ثانية وهنا تعدّ الجريمة العابرة للحدود عائدة للاختصاص الجنائي

للدولة التي ارتُكِبَت بها الجريمة وعائدة للاختصاص الشخصي بالدولة التالية[41]، مما يشكل عائقاً أمام التصدي للإرهاب الإلكتروني، وبَذلت دولة الإمارات العربية المتحدة جهوداً كبيرة في رسم معالم الإرهاب الإلكتروني وقد ورد في المرسوم بقانون اتحادي رقم 34 لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية بدولة الإمارات العربية المتحدة تعريفاً للهجمات الإلكترونية بأنها أي شكل استهدافي للأنظمة المعلوماتية أو البنية التحتية للدولة أو الشبكة الإلكترونية أو وسائل وتقنيات الاتصال والنيل منها لأهداف شخصية أو لأهداف الاختراق أو التسلل أو تعطيل الأنظمة أو غير ذلك[42].

ولكن بالرغم من تلك المعالم إلا أنّه يصعب مراقبة الأفراد في حال الشّك أنهم يحاولون القيام بنشاط إرهابي وهذا عائقاً جديداً أمام التصدّي المُسبق للجرائم الإرهابية، فما تطرّقت له المادة 2 من المرسوم بالقانون الاتحادي رقم 38 لسنة 2022 بإصدار قانون الإجراءات الجزائية في دولة الإمارات العربية المتحدة بعدم القبض على أحد أو وضعهُ تحت المراقبة الإلكترونية إلا بظروف محددة قانوناً[43]، يضع عائقاً أمام مواجهة الإرهاب الإلكتروني حيث أنّ المشرع الإماراتي لم يحدّد ماهية الشروط والأحوال التي يمكن مراقبة الأفراد إلكترونياً للحدّ من مخاطر الجرائم الإرهابية الإلكترونية ولم يحدّد حالات استثنائية تستوجب المراقبة الإلكترونية كحالة الشكّ بقيام الأفراد بجرائم إرهابية إلكترونية، وقد استحدث المشرّع في الإمارات مصطلح الخطورة الإرهابية[44]، وهو الشخص الذي تتوافر فيه أفكار التطرّف والإرهاب ويخشى من ارتكابه لجرائم إرهابية في المستقبل وذكر المشرّع التدابير والإجراءات المتخذة بحقّ الإرهابيين وذلك ضمن المادة 41 من القانون الاتحادي رقم 7 لسنة 2014 في شأن مكافحة الجرائم الإرهابية بدولة الإمارات العربية المتحدة ولكن لم يذكر المشرّع خطورة الإرهاب الإلكتروني والتدابير المذكورة لا تفي بالغرض في حال كان الإرهاب إلكترونياً وبذات الوقت لا يمكن غضّ النظر عن الجرائم الإرهابية الإلكترونية مما يعدّ صعوبة في إمكانية حصر نطاق هذه الظاهرة ومكافحتها.

## المبحث الثاني

## The Second Topic

### الجرائم الإلكترونية الإرهابية: الجزاءات من العقوبات

### Terrorist Cybercrime: Sanctions from Penalties

يعدّ الإرهاب الإلكتروني من الجرائم الإرهابية المعاصرة الأكثر خطورة والعابرة للحدود وجرائم تشكلُ خطورة على أمن الدولة وكيانها وعلى أفرادها وغير محددة بنطاق أو مجال واحد وإنما جرائم متداخلة العوامل السياسية والاقتصادية والاجتماعية والثقافية وغيرها، ويعدّ الإرهاب الإلكتروني من الجرائم الصعب الوصول إليها أو تتمتّع هذه الجرائم بخصائص تجعل السلطات الأمنية غير قادرة على ضبط الجريمة أو

إثبات وقوعها والتحقق منها لأنّ الإرهابي الإلكتروني يتمكّن بسهولة من الوصول لأداة الجريمة كالحاسب الآلي وشبكات الانترنت والمنصّات والمواقع الإلكترونية السهلة الاستخدام وذات الآثار الضّارة والخطرة كالترويع والتخويف والتضليل والتحريض وبثّ الذعر وغيرها من الجرائم التي يصعب ضبطها وملاحقتها[45]، ومن الصعب تحديد الطبيعة الإرهابية الإلكترونية لأنّ أشكال الإرهاب الإلكتروني تتطور بتطور التكنولوجيا والتحديات التقنية تتطور كتحديات القصف الإلكتروني المتمثل بإرسال آلاف الرسائل الإلكترونية إلى موقع الشبكة المستهدفة وزيادة الضغط على قدرتها الاستيعابية لاستقبال الرسائل وتعطيلها أو إيقاف عملها[46]، مما يتطلب تطوير تقنيات الجهات الأمنية لتتمكن من مواجه الإرهاب الإلكتروني، ولكن التقنيات الحديثة وحدها غير قادرة على حماية الأفراد من تهديدات الإرهاب الإلكتروني وما يخلّفه من أضرار وكما نعلم أنّه كلّما كانت الدولة متطورة كلّما ازدادت خطورة الإرهاب الإلكتروني فيها بسبب مهارة وخبرة الإرهابي في استغلال الأجهزة والأدوات التقنية الحديثة واستخدامها في تحقيق مصالحه وما يقابله من نقصٍ في خبرات الجهاز الأمني بالتقنيات التكنولوجية الحديثة.

وازداد انتشار هذه الأشكال الإرهابية الإلكترونية أكثر في الدول التي تعتمد على تقنية المعلومات في أمنها وإدارتها واقتصادها ومن ثمّ كان لابدّ على المجتمع الدولي والمحلي من التعاون والمشاركة وتكثيف الجهود لمواجهتها ووضع استراتيجية موحدة وتشريعات تعرّف الإرهاب الإلكتروني وتحدّد طرق مكافحته، وكما نعلم أنّ أساليب الإرهاب الإلكتروني تختلف باختلاف أسبابه ودوافعه مما يفرض اتخاذ تدابير للتصدّي له وملاحقة مرتكبي العمليات الإرهابية ومعاقبتهم، وبناءً عليه سنقسم المبحث الثاني إلى مطلبين نتحدث في المطلب الأول عن الأساليب المتبعة لملاحقة مرتكبي الجرائم الإلكترونية الإرهابية ونتحدث في المطلب الثاني عن العقوبات القانونية المستحقة على مرتكبي الجرائم الإرهابية الإلكترونية.

## المطلب الأول

## The First Requirement

## أساليب ملاحقة مرتكبي الجرائم الإلكترونية الإرهابية

## Methods of Prosecuting Perpetrators of Terrorist Cybercrimes

إنّ الإرهابيين الإلكترونيين يقومون بالتجسّس على الأشخاص والدّول والهيئات والمؤسّسات عن طريق التقنيات المعلوماتية المعاصرة وشبكة الانترنت ويعدّ التجسّس الخارجي على المواقع السياسية والعسكرية مظهراً من مظاهر الإرهاب الإلكتروني وتحدياً آخر يواجه الدّول وقد أشارت المادة 69 من المرسوم بقانون اتحادي رقم 34 لسنة 2021 بدولة الإمارات العربية المتحدة في شأن مكافحة الشائعات والجرائم

الإلكترونية أنّ أحكام القانون تسري على مرتكب الجرائم من خارج الدولة عندما تكون هذه الجرائم تابعة للنظام المعلوماتي الإلكتروني أو لشبكة المعلومات أو موقع إلكتروني أو أي تقنية خاصة بمؤسسات الدولة[47]،لأنّ هناك فئة متخصصة من المبرمجين تقوم باختراقات غير مشروعة للمواقع الإلكترونية للدول والشبكات بغية الحصول على معلومات هامّة لمؤسسات الدولة أو إضعاف وتدمير البنية التحتية أو المنظومة المعلوماتية أو العسكرية للحكومات[48]، والفضاء الإلكتروني جسّد بيئة ملائمة لأغراض التنظيمات الإرهابية الدعائية وإطلاق الحملات الإعلانية والترويج للأفكار التطرّفية والتكفيرية وجذب المتطوعيّن الشباب للانضمام إلى تنظيماتهم والقتال معهم كما حصل في سوريا والعراق وأفغانستان واليمن وغيرها، مما دفع لتضافر الدّول لمكافحة الإرهاب الإلكتروني ووضع استراتيجية تُعنى بملاحقة الإرهابيين الإلكترونيين وشلّ حركتهم وتفكيك تنظيماتهم والحدّ من آثارهم الضّارة على كافة المستويات الوطنية والعربية والدولية[49].

ومن الوسائل التي استغلها الإرهابيون لنشر أفكارهم والتأثير بالرأي العام القنوات والوسائل الإعلامية التي ساهمت في فشل استراتيجيات الدول وسياساتها الإصلاحية نتيجة دورها الفعّال في المجتمعات والجماهير وإمكانية استخدام هذه الوسائل في العمليات الإرهابية والترويج لها وتصوير الأحداث وإخراجها بحيث تؤثر بالرأي العام لذلك عملت الجهات الأمنية على ملاحقة مرتكبي الجرائم الإرهابية عن طريق تجنيد الخبراء والمتدربين والتقنيين القادرين على متابعة الإرهابيين من خلال منصّات التواصل الاجتماعي والتحقّق من كل ما يقدمه الإعلام من مواد إعلاميّة والتأكد من صحة الاخبار ومضمونها ودلالتها[50].

وكذلك وجد المشرّع في الإمارات العربية المتحدة في المرسوم بقانون اتحادي رقم 55 لسنة 2023 في شأن تنظيم الإعلام تنسيق وضبط المحتويات الإعلامية بما يؤمن البيئة الآمنة للدولة ويعزّز مكانتها العالمية وأكدّ القانون على ضرورة الالتزام بمعايير المحتويات الإعلامية وكيفية ممارسة الأنشطة الإعلامية عبر وسائل الإعلام سواء المسموعة أو المقروءة أو المكتوبة أو الوسائل الإلكترونية أو منصات التواصل الاجتماعي[51].

وإعادة النظر في المحتوى الذي تقدمهُ وسائل الإعلام وفق المعايير التي حددها المشرع في الإمارات العربية المتحدة في المرسوم بقانون اتحادي رقم 55 لسنة 2023 في شأن تنظيم الإعلام[52]، لمعالجة ظاهرة الإرهاب عموماً والإرهاب الإلكتروني خصوصاً لما لها من مخاطر ضارة على أمن الدولة، كما أنّ التصدّي للإرهاب الإلكتروني يتم عن طريق تدمير المعلومات التي ينشرها الإرهابيون على شبكة الانترنت وإغلاق مواقعهم الالكترونية التي تبثّ الذّعر والأفكار المتطرّفة والتجهيز المسبق للتعامل مع الحرب النفسية التي يشنها الإرهابيون ضدّ المواطنين والعامة

والتركيز على إحداث التشريعات التي تتبنّى ملاحقة مرتكبي الجرائم الإلكترونية الإرهابية[53].

وعزّزت الإمارات العربية المتحدة الأمن السيبراني لديها وأحرزت تقدماً في الدفاع ضدّ الهجمات الإرهابية الإلكترونية من خلال مبادرة الأمن السيبراني لحماية المستخدمين والشبكة المعلوماتية من الهجمات السيبرانية وتحصين الفضاء الإلكتروني لديها كما أنشأت فريقاً مختصاً تقنياً للتعامل مع الحوادث الإلكترونية يدعى الفريق الوطني للاستجابة لطوارئ الحاسب الآلي لتقديم الدعم وتحسين معايير حماية أمن المعلومات وإحداث قوانين لمكافحة جرائم المعلومات[54].

وقد أحرزت الدول تقدماً ملحوظاً في السنوات الأخيرة في مجال الأمن الإلكتروني وتأمين بيانات الأفراد وحماية البنية التحتية وتحصين قدراتها الإدارية من الإرهاب الإلكتروني وردع الجريمة الإرهابية الإلكترونية واستحداث تدابير فعّالة لإنفاذ التحقيق في الجرائم العابرة للحدود والملاحقة الدولية للمواقع الإرهابية وتعزيز الاتصال مع الوكالات القانونية وتسهيل إمكانية تبادل المعلومات وإجراء التحقيقات الدولية بالاعتماد على القوانين الوطنية الإجرائية الخاصّة بملاحقة الجرائم الإرهابية ومكافحتها وحث الدول على إغلاق المواقع الإلكترونية الإرهابية[55].

ومن الدول التي أثنت على ملاحقة مجرمي الإرهاب هي الجمهورية المصرية حيث ركز المشرع المصري على مكافحة الإرهاب وخرج عن حدود إقليم الدولة لطالما أنّ الأمر يتعلّق بجرائم تهدّد أمن الدولة وكيانها وأنّ القانون مطبق على المصري أو الأجنبي سواء كان مرتكباً للجريمة أو محرضاً أو متدخلاً أياً كان داخل الأراضي المصرية أو خارجها[56]، لأنّ الدولة حقّها حماية سيادتها وأمنها ونظامها من الجرائم الإرهابية وغيرها.

وعن كيفية الوصول إلى المجرمين عملت دولة الإمارات العربية المتحدة على تنظيم التدابير القانونية والأساليب التقنية اللازمة لمكافحة أشكال الإرهاب والجرائم الإرهابية وقد جاء في قانون حماية البيانات الشخصية لدولة الإمارات العربية المتحدة في المرسوم بقانون اتحادي رقم 45 لسنة 2021 المعايير المفروضة على المتحكم وعلى المعالج وكيفية نقل البيانات الشخصيّة عبر الحدود بهدف المعالجة وكيفية حماية المعلومات الشخصية والإبلاغ عن الانتهاكات والمخالفات[57]، وفي المرسوم بقانون اتحادي رقم 34 في دولة الإمارات العربية المتحدة لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية في المادة 21 تحت عنوان التحبيذ والترويج للجماعات الإرهابية أنّ للمحكمة سلطة إيداع المتهم بدور المناصحة أو وضعه تحت المراقبة الإلكترونية وكذلك منعهُ من استخدام وسائل تقنية المعلومات لفترة محدّدة تقدّرها المحكمة[58].

وكذلك تطرّق المشرّع الإماراتي لاحتمالية وقوع جريمة إرهابية في المستقبل وهنا أيضاً تكمن خطورة الإرهاب الإلكتروني مما يتطلب الاستعانة بالخبراء والفنيين والمختصيّن لدراسة مدى احتمالية وقوع الجريمة الإرهابية من عدمها لاتخاذ التدابير الملائمة[59]، كوضع المتهم تحت المراقبة الإلكترونية أو الحرمان من استخدام الشبكة المعلوماتية أو النظام الإلكتروني أو أي وسيلة تقنية وكذلك يجوز إغلاق الموقع إغلاقاً كلياً أو جزئياً أو حجب الموقع في حال ارتأت المحكمة لذلك كما أنّه يجوز للجهات المختصة إصدار أوامر التصحيح والتعطيل والإيقاف وحظر الوصول للوسائل الإلكترونية [60].

وبدورهِ أيضاً يأتي الذكاء الاصطناعي اليوم كوسيلة تسهم في ملاحقة الجماعات المتطرّفة أو الأشخاص المتورطين في النشاطات الإرهابية سواء كانت في مرحلة التخطيط أو التنفيذ عن طريق تحليل المعطيات والبيانات وتحليل المعلومات والاستفادة من الذكاء الاصطناعي في رصد العمليات ومكانها وأهدافها والتنبؤ بوقوع عمليات مستقبلية وفقاً لنماذج رياضية خاصّة بمعالجة البيانات[61]، والتقنية الأجدر في تتبع وملاحقة عمليات الإرهاب المعقدة نظراً لتطور خوارزمياته البرمجية القادرة على المراقبة والتصوير والتنبؤ بالجرائم ومساهمتها في التّعرف على مقترفي جرائم الإرهاب من خلال التعرّف على هويتهم[62]، وبالرغم من هذه التدابير التي تساهم في الحدّ من الإرهاب الإلكتروني إلّا أنّها لا تغني عن ضرورة تعزيز الدعم التقني للاستخبارات والأجهزة الأمنية القائمة على مواجهة التهديدات الإلكترونية وبناء نظام إلكتروني حكومي جديد قادر على التنبؤ بالتهديدات والتحديات التي قد يستخدمها الإرهابيون الإلكترونيون مستقبلاً والعمل على الحدّ منها، لأنّ هذا النوع من الإرهاب المستحدث لا يمكن حصره ضمن نطاق محدد وقد ينتهك هذا الإرهاب القانون وأمن الدولة بالرغم من التدابير المتخذة للسيطرة عليه، ولذلك وضع المشرع العقوبات اللازمة لمرتكبي هذهِ الجرائم الإرهابية الإلكترونية وهذا ما سنتعرّف عليه في المطلب الثاني العقوبات القانونية على مرتكبي الجرائم الإرهابية الإلكترونية.

## المطلب الثاني

## The Second Requirement

### العقوبات القانونية على مرتكبي الجرائم الإرهابية الإلكترونية

### Legal Penalties for Perpetrators of Cyber Terrorist Crimes

إنّ دول العالم اليوم تواجه تحدياً أمام الجماعات الإرهابية الإلكترونية التي تستغل تطور تقنية المعلومات لتحقيق أغراضها الإرهابية والاعتماد على وسائل اتصال وتقنيات حديثة وتكنولوجية في تنفيذ هجمات غير مشروعة أو أهداف معينة ولكي يوصف المستخدم للإنترنت بأنّه إرهابي إلكتروني وليس مخترقاً فقط فلابدَّ أن تسبب هجماته الضّرر والأذى للأشخاص أو المؤسسات أو الحكومات أو أي أشكال الأذى

الإرهابي وهو ما يميّز جرائم الإرهاب الإلكتروني عن غيرها من الجرائم وفي الواقع الإرهاب الإلكتروني من المسائل القانونية التي يتعيّن التركيز عليها في النظام القانوني الدولي والمحلي وتحديد ماهية هذا الإرهاب سواء من الناحية الإجرائية أو العقابية[63]، وتطوير المهارات الدفاعية لمواجهة الهجمات الإرهابية والاستعانة بأصحاب الخبرات وتحصين البنية التحتية للدولة وتدريب القدرات والكفاءات للأجهزة الأمنية الوطنية ودعم برامج الأمان والحماية من جرائم الإرهاب وتفعيل دور الأفراد في استخدام أنظمة الأمان والحماية الإلكترونية وحثّهم على إخفاء بياناتهم وتشفيرها وإعلام الجهات المختصة بأي نشاط إرهابي يمكن أن يشعر به المستخدمين سواء كان هذا النشاط يتعلّق بفرد أو مؤسسة والإبلاغ عن أي عمليات تشويش أو تعطيل للأجهزة الآلية، كل تلك التدابير وردت في القانون اتحادي رقم 7 لدولة الإمارات العربية المتحدة في شأن مكافحة الجرائم الإرهابية لسنة 2014م، والمرسوم بقانون اتحادي لدولة الإمارات العربية المتحدة بإصدار قانون الإجراءات الجزائية رقم 38 لسنة 2022م[64]، ومكافحة الإرهاب الإلكتروني مسؤولية تتطلّب المشاركة والتعاون والتنسيق والاستعداد الكامل لمواجهة الأشكال المستحدثة من جرائم الإرهاب الإلكتروني وعدم التهاون مع مرتكبي هذه الجرائم بل ومعاقبة المقترفين ومحاكمتهم.

وعليه نظّمت دولة الإمارات العربية المتحدة عقوبات قانونية مستحقّة للإرهابيين المستغلين للمواقع الإلكترونية وتقانة المعلومات بغرض الترويج والتحبيذ للانضمام للجماعات الإرهابية وممارسة النشاطات الإرهابية التخريبية وقد ورد في المادة 21 من المرسوم بقانون اتحادي رقم 34 لدولة الإمارات العربية المتحدة لسنة 2021م في شأن مكافحة الشائعات والجرائم الإلكترونية عقوبة السجن المؤبد وغرامة مالية من مليوني درهم إلى أربعة ملايين درهم لكل من يقدم على إنشاء أو إدارة أو الإشراف على المواقع الإلكترونية الخاصة بالمجموعات الإرهابية أو كل من يقوم بنشر بيانات أو معلومات على شبكة الإنترنت أو وسائل تقنية تابعة لمجموعات إرهابية أو منظمات أو هيئات غير مشروعة بهدف جذب الأعضاء أو الترويج أو التمويل للأنشطة والأعمال الإرهابية وكذلك بالنسبة لنشر أساليب وطرق تصنيع الذخائر والمتفجرات والأسلحة أو نشر طرق تصنيع المواد السامة والخطرة[65].

وكذلك الشأن بالنسبة لإجراءات وضع المتهم تحت المراقبة الإلكترونية فقد جاء في المرسوم بقانون اتحادي رقم 38 في دولة الإمارات العربية المتحدة بإصدار قانون الإجراءات الجزائية لسنة 2022م أحكام المراقبة وآلية تنفيذه المراقبة وتنظيم عمليات المراقبة عن بُعد[66]، وجاء في المرسوم بقانون اتحادي رقم 34 في دولة الإمارات العربية المتحدة في شأن مكافحة الشائعات والجرائم الإلكترونية لسنة 2021م عقوبة كل من ينشئ موقعاً إلكترونياً أو محتوىً رقمياً أو كل من يدير أو يستخدم شبكة الإنترنت أو وسائل تقانة المعلومات لأغراض تحريضية أو عنصرية أو بغرض

الإخلال بالوحدة الوطنية وبث أفكار مخلّة بالأمن والنظام العام بالدولة وتكون العقوبة هي السجن المؤقت أو الغرامة المالية من مائتي ألف درهم إلى مليون درهم لمقترفي هذه الأعمال[67].

وأيضاً بالنسبة للجرائم التي ترتكب عن طريق وسائل الاتصال والتقنيات المعلوماتية والمواقع الإلكترونية للنيل من المقدسات الدينية أو الإساءة للشعائر الإسلامية أو أحد الأديان السماوية أو التحريض على المعصية أو أي أذية دينية تنال من الذات الإلهية كُلها تعد جرائم يعاقب عليها القانون وجاء ذلك في المرسوم بقانون اتحادي رقم 34 في دولة الإمارات العربية المتحدة في شأن مكافحة الشائعات والجرائم الإلكترونية لسنة 2021م بالحبس والغرامة المالية من مائتين وخمسين ألف درهم إلى مليون درهم وقد تصل العقوبة أحياناً إلى السجن المؤقت لسبع سنوات لمرتكبي هذه الجرائم[68].

وعلى الرغم من القوانين السابقة والتدابير التي اتخذتها الدول والإجراءات الخاصة بأساليب ملاحقة مرتكبي العمليات الإرهابية الإلكترونية إلا أنّ ذلك لم يمنع الإرهابيين من القيام بعملياتهم الإرهابية حتى اليوم بل على العكس فقد ازدادت العمليات الإرهابية لدرجة خطرة والدول باتت غير قادرة على توقع الهجمات السيبرانية والإرهابية الإلكترونية التي قد تتعرّض لها مستقبلاً ونرى أنّ الدول تتطلّب إحداث نظام قانوني متكامل ومنفصل خاص بالإرهاب الإلكتروني يتضمن أساليب تقنية إلكترونية حديثة للتعامل مع الإرهاب الإلكتروني وإحداث هيئة دولية معنية بمكافحة الإرهاب الإلكتروني وفرض عقوبات على الدول التي تساهم في دعم العمليات الإرهابية.

## الخاتمة

## Conclusion

ظاهرة الجرائم الإرهابية الإلكترونية تطورت مع تطور التقنيات المعلوماتية والتكنولوجية وأصبح الإرهابيون يعتمدون على الشبكة المعلوماتية لتنفيذ مخططاتهم الإجرامية، واتخذ الإرهاب منحىً جديداً مختلفاً عن الإرهاب التقليدي بالإمكانيات التي يوفرها المجال الإلكتروني لارتكاب جرائم كالنعف والتحريض والتضليل وغيرها من الجرائم المعروفة واستحداث جرائم لم يكن يشهدها العالم مسبقاً وأساليب وهجمات إلكترونية جديدة، مما وضع الجهات الأمنية أمام صعوبات من ناحية إثبات الجرم الجنائي فمن غير الممكن فحص مسرح الجريمة كما في جرائم الإرهاب التقليدي للبحث عن آثار للمجرمين لأنّ الجرائم التي تُرتكب عن طريق الشبكات المعلوماتية قد لا يترتب عليها أيّة آثار مادية، ومن الناحية القانونية يكون عدم تناسق التشريعات بين الدول بشأن الإرهاب الإلكتروني سبباً رئيساً بجعل المجرمين بمنأى عن العدالة وأيضاً قد يكون الفاعلين خارج نطاق الدولة مما يساهم في إفلاتهم من العقاب وقد عملت الجهات الأمنية على ملاحقة مرتكبي الجرائم الإرهابية عن طريق تجنيد الخبراء والمتدربين والتقنيين القادرين على متابعة الإرهابيين من خلال منصّات التواصل الاجتماعي والتحقّق من كل ما يقدمه الفضاء الإلكتروني من مواد ومحتويات وفرض عقوبات صارمة على المخالفين.

**النتائج:**

1. إنّ الاختلاف ما بين الإرهاب الإلكتروني والإرهاب التقليدي يكمن في اعتماد الإرهاب التقليدي على الوسائل المادية كالأسلحة والقنابل والمتفجرات والطائرات والمدرعات والدبابات وغيرها من الوسائل ذات الأثر المباشر في أرض الواقع أما الإرهاب الإلكتروني يعتمد أساساً على استخدام أدوات رقمية مرتبطة بالإنترنت والمعلوماتية والمنصّات والمواقع الإلكترونية سهلة الوصول إليها وبدون أن تحدث أثراً، ويكون من الصعب على الجهات الأمنية الوصول لمقترفيها أو كشفها أو ضبطها وقد تكون هذه الجرائم عابرة للحدود مما يزيد الأمر صعوبة.
2. إنّ الدول لا تزال تعاني افتقاراً في تحصين الفضاء الإلكتروني الخاص ببياناتها وبيانات الأفراد والأدلة الجنائية التقليدية تجد صعوبات من ناحية إثبات الجرم الجنائي في الجرائم الإرهابية الإلكترونية لأنّه غير الممكن فحص مسرح الجريمة كما في جرائم الإرهاب التقليدي لأنّ الجرائم التي ترتكب عن طريق الشبكات المعلوماتية والذكاء الصناعي قد لا يترتب عليها أيّة آثار مادية بل يمكن دخول أعداد من المستخدمين للشبكة والتغيير أو العبث بمجريات الجريمة وزوال آثارها.

3. الصعوبات القانونية التي تواجه كشف الإرهاب الإلكتروني وملاحقته أنّ القانون الجنائي يطبّق وفق الأوضاع والمعايير التي كانت سائدة وقت وضع هذا القانون ولكن هذا القانون لا يتناسب مع التطور التكنولوجي اليوم لأنّ القانون الجنائي لا يتطور بذات السرعة التي تتطور بها التقنيات المعلوماتية الحديثة، وكذلك عدم تناسق التشريعات بين الدول بشأن الإرهاب الإلكتروني يجعل المجرمين بمنأى عن العدالة لأنّه لا يوجد نموذج موحد لتطبيق أحكام جزائية لمكافحة الإرهاب الإلكتروني وذلك بسبب الاختلاف بثقافات الشّعوب وعاداتهم وتقاليدهم حول العالم وما يكون مباحاً في إحدى الدول قد يكون إجراماً في دولة أُخرى.
4. تواجه السلطات الأمنية تحديات أمام مواجهة الإرهاب الإلكتروني في اختلاف الإجراءات الجزائية المُتخذة في متابعة النشاط الإرهابي كالتفتيش والتحقيق والمحاكمة وطرق جمع الدلائل والإثبات من دولة لأخرى، كوضع المتهم تحت المراقبة الإلكترونية أو الحرمان من استخدام الشبكة أو إغلاق الموقع ويجوز للجهات المختصة إصدار أوامر التصحيح والتعطيل والإيقاف وحظر الوصول للوسائل الإلكترونية، أو ملاحقة الجماعات المتطرّفة عن طريق الذكاء الاصطناعي والتنبؤ بوقوع عمليات مستقبلية وفقاً لنماذج رياضية خاصّة بمعالجة البيانات.

**التوصيات:**

1. نوصي المجتمع الدولي بالسعي لوضع تعريف موحد للإرهاب الإلكتروني تتفق عليه جميع دول العالم وتحديد أساليب هذا الإرهاب والسعي لتطوير هذا التعريف الموحد وفقاً للتطور الذي تتطور به التكنولوجيات الحديثة وإدراج الأساليب الجديدة التي تتعرّض لها الدول ضمن التعريف خلال كلّ ستة أشهر أو كُل عام على سبيل المثال.
2. نهيب بالجهات الأمنية التنسيق مع كافة الوزارات والتعاون مع المبرمجين والمختصيّن بالمجالات الإلكترونية والتقنية لتطوير قدرات ومهارات الأدلة الجنائية والجهات المختصّة ووضعها بصورة التطورات التقنية التي تحصل على مستوى العالم وإعداد متدربين وأنظمة حماية وأمان قادرة على حماية أمن الدولة واستقرارها من الهجمات الإلكترونية الإرهابية، وتزويد الجهات الأمنية بأساليب الذكاء الصناعي القادرة على تتبع مرتكبي الجرائم الإرهابية أو التنبؤ بوقوعها مستقبلاً.
3. ننصح بتحديث قانون مكافحة الجرائم الإرهابية في الإمارات العربية المتحدة وتخصيص مادة قانونية خاصة بجرائم الإرهاب الإلكتروني تتضمن تعريف الإرهاب الإلكتروني وطرق ملاحقته والعقوبات المستحقة لمرتكبي هذه الجرائم وذلك للتفرقة بين الجرائم الإرهابية الإلكترونية وجرائم الاختراق الإلكتروني ونقترح النص التالي "جرائم الإرهاب الإلكتروني هي كل جريمة ترتكب باستعمال الوسائل الإلكترونية أو منصات التواصل عبر

الشبكة بغرض الترهيب أو بثّ الأفكار الإرهابية المتطرفة أو التحريض على العنف أو التخريب، ومن يُشتبه بخطورة قيامه بأعمال إرهابية إلكترونية يوضع تحت المراقبة الإلكترونية أو قد يحرم من استخدام الشبكات المعلومات وفق الظروف التي تقتضيها الحالة وفي حال ثبت قيامه بالأعمال الإرهابية عن طريق التقنيات الإلكترونية يعاقب بالحبس والغرامة المالية المقدرة حسب الجريمة ويحجب الموقع الذي يستخدمه".

4. ندعو الجهات الأمنية إلى توحيد إجراءات التتبع بحق مجرمي الإرهاب الإلكتروني أو المتهمين بهذه الجرائم وتوحيد طرق التحقيق والتفتيش والمحاكمة على الصعيد الوطني والدولي لأنّ الجرائم العابرة للحدود تتطلّب ملاحقتها التعاون من أكثر من دولة وتضافر جهود المنظمات الدولية أيضاً.

## الهوامش
## Endnotes

[1]إنجى المهدى، الإرهاب الإلكتروني: الظاهرة والتداعيات الاستخدام من قبل التنظيمات الجهادية، المجلة الاجتماعية القومية، المجلد الثامن والخمسين، العدد الأول، يناير 2021م، وجاء فيه تعريف الإرهاب الإلكتروني بأنه: "هجمة إلكترونية غرضها تهديد الحكومات أو العدوان عليها، سعياً لتحقيق أهداف سياسية أو دينية أو أيديولوجية، وتنتج عنها آثار تخريبية مدمرة مكافئة لآثار الأفعال المادية للإرهاب"، ص 39.

[2] انظر القانون اتحادي، رقم 7، دولة الإمارات العربية المتحدة، في شأن مكافحة الجرائم الإرهابية، لسنة 2014م، وكذلك مرسوم بقانون اتحادي، رقم 34، دولة الإمارات العربية المتحدة، في شأن مكافحة الشائعات والجرائم الإلكترونية، لسنة 2021م.

[3] انظر الأمم المتحدة UNODC، نيويورك، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، فيينا، استخدام الانترنت في أغراض إرهابية، حزيران 2013م، وجاء فيه "إنّ استخدام الإنترنت في أغراض إرهابية ظاهرة تتفشّى بسرعة، وتتطلّب من الدول الأعضاء أخذ زمام المبادرة للتصدّي لها بالتنسيق فيما بينها"، ص v.

[4] انظر الأمم المتحدة UNODC، نيويورك، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، فيينا، استخدام الانترنت في أغراض إرهابية، المرجع نفسه، وجاء فيه في استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب، ولا سيما بإقرارها بأنّ "اتخاذ تدابير فعّالة لمكافحة الإرهاب وحماية حقوق الإنسان هدفان لا يتعارضان، بل متكاملان ويعزّز كل منهما الآخر"، ص19.

[5] ملامح التحول العالمي إلى مرحلة "ما بعد المعلومات"، متاح على الموقع الإلكتروني، https://futureuae.com/ar/Mainpage/Item/4267 ، آخر تاريخ للزيارة 2024/11/29م.

[6] انظر القانون اتحادي، رقم 7، دولة الإمارات العربية المتحدة، في شأن مكافحة الجرائم الإرهابية، لسنة 2014م.

[7] مرسوم بقانون اتحادي، رقم 20، دولة الإمارات العربية المتحدة، في شأن مواجهة جرائم غسل الأموال ومكافحة تمويل الإرهاب وتمويل التنظيمات غير المشروعة، لسنة 2018م.

[8] انظر مرسوم بقانون اتحادي، رقم 34، دولة الإمارات العربية المتحدة، في شأن مكافحة الشائعات والجرائم الإلكترونية، لسنة 2021م.

[9] انظر قرار رئيس جمهورية مصر العربية، بالقانون رقم 94، لسنة 2015، بإصدار قانون مكافحة الإرهاب، موجود في الجريدة الرسمية، العدد 33، 15 أغسطس سنة 2015.

[10] انظر مرسوم بقانون اتحادي، رقم 20، دولة الإمارات العربية المتحدة، في شأن مواجهة جرائم غسل الأموال ومكافحة تمويل الإرهاب وتمويل التنظيمات غير المشروعة، لسنة 2018م، المادة 4 وجاء فيها "يكون الشخص الاعتباري مسؤولاً جزائياً عن الجريمة إذا ارتكبت باسمه أو لحسابه عمداً، وذلك دون الإخلال بالمسؤولية الجزائية الشخصية لمرتكبها والجزاءات الإدارية المنصوص عليها قانوناً".

[11] انظر الأمم المتحدة UNODC، نيويورك، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، فيينا، استخدام الانترنت في أغراض إرهابية، المرجع السابق، وجاء في قرار الجمعية العامة

178/66 واضطلع فرع منع الإرهاب التابع للمكتب، في إطار أداء الولاية المسندة إليه في "تطوير المعارف القانونية المتخصصة في مجال مكافحة الإرهاب .... وتقديم المساعدة لمن يطلبها من الدول الأعضاء ..... لتعزيز قدرة نظم العدالة الجنائية على مواجهة الإرهاب، بما في ذلك.... استخدام شبكة الإنترنت لأغراض إرهابية"، ص 36.

(12) حسام فايز عبد الحي، الإرهاب الإلكتروني كوسيلة للحرب النفسية، دراسة تأصيلية نظرية، مجلة البحوث في مجالات التربية النوعية، العدد الثالث عشر، 2017م، ص 76 -75.

(13)انظر مرسوم بقانون اتحادي، رقم 34، دولة الإمارات العربية المتحدة، في شأن مكافحة الشائعات والجرائم الإلكترونية، لسنة 2021م، المادة 60 وجاء في البند 3 "ارتكاب الجاني أي جريمة منصوص عليها في هذا المرسوم بقانون لحساب أو لمصلحة دولة أجنبية أو أي جماعة معادية أو جماعة إرهابية أو تنظيم غير مشروع".

(14) انظر الأمم المتحدة UNODC، نيويورك، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، فيينا، استخدام الانترنت في أغراض إرهابية، المرجع السابق، ص11-10 .

(15) انظر مرسوم بقانون اتحادي، رقم 34، دولة الإمارات العربية المتحدة، في شأن مكافحة الشائعات والجرائم الإلكترونية، لسنة 2021م، المادة 60 الظروف المشددة في تطبيق أحكام هذا المرسوم بقانون يعدّ ظرفاً مشدداً: البند 2 وجاء فيه "استخدام الجاني شبكة المعلومات أو أي نظام معلوماتي إلكتروني أو موقع إلكتروني أو أي وسيلة تقنية معلومات عند ارتكاب أي جريمة لم ينص عليها هذا المرسوم بقانون".

(16) إنجى المهدى، الإرهاب الإلكتروني: الظاهرة والتداعيات الاستخدام من قبل التنظيمات الجهادية، المرجع السابق، ص37- ص 42.

(17) انظر مرسوم بقانون اتحادي، رقم 34، دولة الإمارات العربية المتحدة، في شأن مكافحة الشائعات والجرائم الإلكترونية، لسنة 2021م، المادة 65، حجية الأدلة وجاء فيها "يكون للأدلة المستمدّة أو المستخرجة من الأجهزة أو المعدات أو الوسائط أو الدعامات الإلكترونية أو النظام المعلوماتي أو برامج الحاسب أو من أي وسيلة لتقنية المعلومات حجية الأدلة الجنائية المادية في الإثبات الجنائي".

(18) لالوسوفريادي بن مجيب، الإعلام الجديد في مواجهة تحديات الإرهاب الإلكتروني، الزهراء مجلة نصف سنوية محكمة، السنة السابعة عشرة، العدد 1، 2020م، ص 239-237.

(19) انظر مرسوم بقانون اتحادي، رقم 20، دولة الإمارات العربية المتحدة، في شأن مواجهة جرائم غسل الأموال ومكافحة تمويل الإرهاب وتمويل التنظيمات غير المشروعة، لسنة 2018م، وجاء في تعريف تمويل التنظيمات غير المشروعة: هو "كل فعل مادي أو تصرّف قانوني يراد به توفير المال لتنظيم غير مشروع أو لأحد أنشطته أو لأحد المنتمين إليه".

(20) انظر قرار رئيس جمهورية مصر العربية، بالقانون رقم 94، لسنة 2015، بإصدار قانون مكافحة الإرهاب، موجود في الجريدة الرسمية، العدد 33، 15 أغسطس سنة 2015، المادة 3، وجاء فيها "يقصد بتمويل الإرهاب كل جمع أو تلقي أو حيازة أو إمداد أو نقل أو توفير أموال أو أسلحة أو ذخائر أو مفرقعات أو مهمات أو آلات أو بيانات أو معلومات أو مواد أو غيرها، بشكل مباشر أو غير مباشر، وبأية وسيلة كانت بما فيها الشكل الرقمي أو الإلكتروني، وذلك بقصد استخدامها، كلها أو

بعضها في ارتكاب أية جريمة إرهابية أو العلم بأنها ستستخدم في ذلك، أو بتوفير ملاذ آمن لإرهابي أو أكثر، أو لمن يقوم بتمويله بأي من الطرق المتقدم ذكرها".

(21) محمد خليفة محمد سليمان الهنائي ونزار محمد أحمد، دور الذكاء الاصطناعي في مكافحة جريمة تمويل الإرهاب الإلكتروني، بيردانا، المجلة الدولية للبحوث الأكاديمية، العلوم الاجتماعية والإنسانية، المجلد 19، العدد 1، 2024م، وجاء فيها "من المعروف أن الجماعات الإرهابية تستخدم الذكاء الاصطناعي لعمل فيديوهات وصور تروج لأفكارها الإرهابية لجذب تعاطف المستخدمين العاديين"، ص 73.

(22) السر الجيلاني الأمين حماد ومحمد نصر عبد الله نصر، مفهوم الإرهاب الالكتروني وطرق مكافحته، مجلة قضايا التطرّف والجماعات المسلحة، المجلد 04، العدد 11، 2023، وجاء فيها "البيئة الهادئة: مما يدل على خطورة الارهاب الالكتروني انه يتم في بيئة هادئة لا يلتفت اليها أحد. وتصعب عملية المراقبة فيمكن ان تكتمل كل اركان الجريمة الارهابية الالكترونية. ولا يعرفها أحد إلّا بعد عملية التنفيذ"، ص 336.

(23) محمد حمدي عبد العليم علام، الإثبات الجنائي في جرائم الإرهاب الإلكتروني، مجلة قضايا التطرف والجماعات المسلحة، المجلد 04، العدد 11، 2023م، ص 216 – 214.

(24) مرسوم بقانون اتحادي، رقم 34، دولة الإمارات العربية المتحدة، في شأن مكافحة الشائعات والجرائم الإلكترونية، لسنة 2021م، المادة 44، 59، 62.

(25) انظر قرار مجلس النواب القانوني، جمهورية مصر العربية، بالقانون رقم 175، لسنة 2018، في شأن مكافحة جرائم تقنية المعلومات، موجود في الجريدة الرسمية، العدد 32، 14 أغسطس سنة 2018، المادة 2، 24، 25.

(26) مرسوم بقانون اتحادي، رقم 34، دولة الإمارات العربية المتحدة، في شأن مكافحة الشائعات والجرائم الإلكترونية، لسنة 2021م، المادة 1.

(27) سليماني مباركة، الإرهاب الإلكتروني وطرق مكافحته، مجلة الحقوق والعلوم السياسية، العدد 08، المجلد01، 2017م، ص 352-350.

(28) ناصر العلي، الجهود الدولية في مكافحة الإرهاب الإلكتروني، مجلة الباحث للدراسات الأكاديمية، المجلد 08، العدد01، السنة 2021، ص 41-40.

(29) محمد الطيب عبد الله خالد، الإرهاب الإلكتروني، مجلة كلية الشريعة والقانون، المجلد 13، 2020م، ص 107- ص 108.

(30) مصطفى خليل كامل خليل، جرائم الإرهاب الإلكتروني من منظور القانون الدولي، مجلة كلية الحقوق، المجلد الخامس، العدد الثاني، ديسمبر 2022، ص15.

(31) الأمم المتحدة المكتب المعني بالمخدرات والجريمة، دراسة حول تشريعات مكافحة الإرهاب في دول الخليج العربية واليمن، فيينا، 2009، ص 3-1.

(32) مصطفى خليل كامل خليل، جرائم الإرهاب الإلكتروني من منظور القانون الدولي، المرجع نفسه، ص56.

(33) مرسوم بقانون اتحادي، رقم 20، دولة الإمارات العربية المتحدة، في شأن مواجهة جرائم غسل الأموال ومكافحة تمويل الإرهاب وتمويل التنظيمات غير المشروعة، لسنة 2018م.

(34) انظر قرار رئيس جمهورية مصر العربية، بالقانون رقم 94، لسنة 2015، بإصدار قانون مكافحة الإرهاب، موجود في الجريدة الرسمية، العدد 33، 15 أغسطس سنة 2015.

(35) سليماني مباركة، الإرهاب الإلكتروني وطرق مكافحته، المرجع السابق، ص350 - ص355.

(36) محمود سلامة، المنظمات الدولية والإقليمية في مكافحة الإرهاب الإلكتروني، مقال في السياسة الدولية، يناير 2022، موجود على الموقع الرسمي https://www.researchgate.net/publication/357578485، ص3-2.

(37) ناصر العلي، الجهود الدولية في مكافحة الإرهاب الإلكتروني، المرجع نفسه، وجاء فيها "المعاهدة الدولية الوحيدة ذات الطابع الإقليمي التي تتناول جزئياً قضايا مكافحة الإرهاب الإلكتروني هي الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الصادرة في 21 ديسمبر 2010، تسرد المادة 15 الجرائم المتعلّقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات: 1- تنشر أفكار ومبادئ جماعات إرهابية والدعوة لها. 2 – تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية. 3 – نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية. 4- نشر النعرات والفتن والاعتداء على الأديان والمعتقدات"، ص 34.

(38)ناصر العلي، الجهود الدولية في مكافحة الإرهاب الإلكتروني، المرجع نفسه، ص 41 – ص42.

(39) خالد جمعة سبيت احمد المخمري، المواجهة الأمنية للإرهاب الإلكتروني، مجلة البحوث القانونية والاقتصادية، المجلد 58، العدد2، أكتوبر 2023، وجاء فيه "من خلال تعاطي الأنظمة القانونية القائمة في كثير من الدول نجد أنها لا تملك اتفاقا عاماً مشتركاً حول صور إساءة استخدام نظم المعلومات وشبكة الإنترنت الواجب تجريمها، فما هو مباح في أحد الأنظمة نجدهُ إجراماً في غيرها والعكس بالعكس وهذا يرجع لعدة أسباب وعوامل منها على سبيل المثال لا الحصر: الظروف، العادات، التقاليد والثقافات التي تختلف من مجتمع لآخر وبذلك تختلف التشريعات وفقاً لذلك"، ص 398.

(40) خالد جمعة سبيت احمد المخمري، المواجهة الأمنية للإرهاب الإلكتروني، المرجع نفسه، وجاء فيه "فبعض الدول تجد أنها مكبلة بقوانينها المحلية في عملية إنقاذ القانون مما يعيق ما تطلبه منها الدولة الاخرى فيضيع عنصر التعاون بينهما فقد لا يسمح بإثبات الأدلة أو حتى تسليمها لدولة ما بحكم أن القانون المحلي لا يسمح بذلك حتى ولو كان في اختصاص قضائي وبشكل مشروع"، ص399.

(41) خالد جمعة سبيت احمد المخمري، المواجهة الأمنية للإرهاب الإلكتروني، المرجع نفسه، وجاء "فقد نرتكب جريمة في إقليم دولة معينة من قبل أجنبي فالجريمة تكون خاضعة للاختصاص الجنائي بالدولة الأخرى استنادا إلى مبدأ الإقليمية وتخضع لاختصاص الدولة التالية على أساس مبدأ الاختصاص الشخصي، والجريمة قد تهدد أمن وسلامة دولة أخرى وتدخل عند ذلك في اختصاصها استنادا إلى مبدأ العينية"، ص400.

(42) انظر مرسوم بقانون اتحادي، دولة الإمارات العربية المتحدة، بشأن مكافحة الشائعات والجرائم الإلكترونية، رقم 34، لسنة 2021، وجاء فيه " الهجمات الإلكترونية: كل استهداف متعمد ومخطط للأنظمة المعلوماتية أو البنية التحتية أو الشبكات الإلكترونية أو وسائل تقنية المعلومات يقلل من قدرات ووظائف أي منها، سواء كان ذلك لغرض شخصي أو لأغراض الاعتراض أو التسلل أو

الاختراق أو التسريب أو بغرض تعريض البيانات أو المعلومات للخطر أو تعطيل العمليات وما في حكمها".

(43) انظر مرسوم بقانون اتحادي، دولة الإمارات العربية المتحدة، بإصدار قانون الإجراءات الجزائية، رقم 38، لسنة 2022، الباب التمهيدي، المادة 2، وجاء فيها "لا يجوز القبض على أحد أو تفتيشه أو حجزه أو حبسه أو منعه من السفر أو وضعه تحت المراقبة الإلكترونية إلا في الأحوال وبالشروط المنصوص عليها في القانون، ولا يتم الحجز أو الحبس إلا في الأماكن المخصّصة لكل منها وللمدة المحدّدة في الأمر الصادر من السلطة المختصة".

(44) انظر القانون الاتحادي، رقم 7، دولة الإمارات العربية المتحدة، في شأن مكافحة الجرائم الإرهابية، لسنة 2014م، المادة 40، وجاء فيها "تتوفر الخطورة الإرهابية في الشخص إذا كان متبنياً للفكر المتطرّف أو الإرهابي بحيث يخشى من قيامه بارتكاب جريمة إرهابية".

(45) محمد الطيب عبد الله خالد، الإرهاب الإلكتروني، المرجع السابق، ص 102.

(46) انظر هشام بشير، أراء حول الخليج، الإرهاب الإلكتروني في ظلّ ثورة المعلومات، العدد 92، أيار 2012، موجود على الموقع الالكتروني https://mail.araa.sa/index.php?option=com_conten&view=article&id=244:20 14-06-13-16-21-31&catid=132&Itemid=294 تاريخ آخر زيارة2024/11/29.

(47)انظر مرسوم بقانون اتحادي، رقم 34، دولة الإمارات العربية المتحدة، في شأن مكافحة الشائعات والجرائم الإلكترونية، لسنة 2021م، المادة69، وجاء فيها "مع عدم الإخلال بأحكام قانون العقوبات المشار إليه، تسري أحكام هذا المرسوم بقانون على كل من ارتكب إحدى الجرائم الواردة به خارج الدولة في الأحوال الآتية: 1.إذا كان محلها نظام معلوماتي إلكتروني أو شبكة معلوماتية أو موقع إلكتروني أو وسيلة تقنية معلومات خاصّة أو عائدة لإحدى مؤسسات الدولة".

(48) انظر مخترق، متاح على الموقع الإلكتروني، https://ar.m.wikipedia.org/wiki/%D9%85%D8%AE%D8%AA%D8%B1%D9%82 ، تاريخ آخر زيارة 2024/11/29م.

(49) خالد جمعة سبيت احمد المخمري، المواجهة الأمنية للإرهاب الإلكتروني، المرجع السابق، ص 386.

(50) لالوسوفريادي بن مجيب، الإعلام الجديد في مواجهة تحديات الإرهاب الإلكتروني، المرجع السابق، وجاء فيه "استعمل الارهابيون وسائل الإعلام وتقنيات التواصل الحديثة في ربط الشبكات الإرهابية والتخطيط للعمليات العدوانية، وتغطيتها بتقنيات عالية في التصوير والإخراج للترويج لها وقد أصبحت الجهات الأمنية المختصة في ملاحقة الإرهابيين تجند خبراء متمرسين، لمتابعتهم عبر شبكات التواصل الاجتماعي وتحليل ما يصدرونه من مواد إعلامية للتحقق من مضامينها ودلالاته"، ص 239.

(51) انظر مرسوم بقانون اتحادي، رقم 55، دولة الإمارات العربية المتحدة، في شأن تنظيم الإعلام، لسنة 2023م، المادة 3، 6، 8، 9.

(52) انظر مرسوم بقانون اتحادي، رقم 55، دولة الإمارات العربية المتحدة، في شأن تنظيم الإعلام، لسنة 2023م، المادة 17.

(53) خالد جمعة سبيت احمد المخمري، المواجهة الأمنية للإرهاب الإلكتروني، المرجع السابق، وجاء فيه "وتتطلب أيضاً مقاومة الإرهاب التصدّي للمعلومات المدمرة على الشبكة العنكبوتية لمعالجتها من خلال سن التشريعات المتكفلة بإغلاق هذه المواقع التي تقوم بترويج الأفكار المتطرفة وخصوصاً تلك المواقع التي تدّعي نسبها وانتمائها للدين الإسلامي الحنيف، ومع ذلك لابد من تجهيز نموذج شامل للاتصال لمجابهة الحرب النفسية التي تقوم بشنها المجموعات الإرهابية"، ص 388.

(54) انظر البوابة الرسمية لحكومة دولة الإمارات العربية المتحدة، السلامة السيبرانية والأمن الرقمي، متاح على الموقع الإلكتروني، https://u.ae/ar-ae/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security/cyber-safety ، تاريخ آخر زيارة 2024/11/29م.

(55) لمياء محمد عبد السلام جودة، دور المنظمة الدولية للشرطة الجنائية في مكافحة جريمة الإرهاب الدولي، مجلة البحوث الفقهية والقانونية، العدد الثاني والأربعين، 2023م، ص 222-223.

(56) قرار رئيس جمهورية مصر العربية، بالقانون رقم 94، لسنة 2015، بإصدار قانون مكافحة الإرهاب، موجود في الجريدة الرسمية، العدد 33، 15 أغسطس سنة 2015، المادة 2.

(57) انظر مرسوم بقانون اتحادي، رقم45، دولة الإمارات العربية المتحدة، بشأن حماية البيانات الشخصية، لسنة 2021م، المادة 7، 8، 9، 11، 13، 22.

(58) انظر مرسوم بقانون اتحادي، رقم 34، دولة الإمارات العربية المتحدة، في شأن مكافحة الشائعات والجرائم الإلكترونية، لسنة 2021م، المادة 21، البند 3، وجاء فيه " للمحكمة في-غير حالات العود-بدلاً من الحكم بالعقوبة المشار إليها في الفقرة (2) من هذه المادة أن تحكم بإيداع المتهم إحدى دور المناصحة أو الحكم بوضعه تحت المراقبة الإلكترونية ومنعه من استخدام أياً من وسائل تقنية المعلومات خلال فترة تقدّرها المحكمة على ألا تزيد على الحدّ الأقصى للعقوبة المقرّرة.

(59) انظر مرسوم بقانون اتحادي، رقم 34، دولة الإمارات العربية المتحدة، في شأن مكافحة الشائعات والجرائم الإلكترونية، لسنة 2021م، المادة 59.

(60)انظر مرسوم بقانون اتحادي، رقم 34، دولة الإمارات العربية المتحدة، في شأن مكافحة الشائعات والجرائم الإلكترونية، لسنة 2021م، المادة62.

(61) محمد خليفة محمد سليمان الهنائي ونزار محمد أحمد، دور الذكاء الاصطناعي في مكافحة جريمة تمويل الإرهاب الإلكتروني، المرجع السابق، ص 70.

(62) محمد خليفة محمد سليمان الهنائي ونزار محمد أحمد، دور الذكاء الاصطناعي في مكافحة جريمة تمويل الإرهاب الإلكتروني، المرجع السابق، وجاء فيه "توفر تقنية الذكاء الاصطناعي فوائد عديدة في مختلف مجالات الحياة، وخاصة في مكافحة التطرف والإرهاب؛ حيث تلعب دوراً إيجابياً مهماً، وتتمثل أهم هذه الفوائد في تقليل الوقت والجهد المبذولين في عمليات البحث والتتبع، خاصة مع تزايد حجم المعلومات المعاجلة وتعقيدها وتشابكها. وتعدّ 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"، ص 71.

(63) مصطفى خليل كامل خليل، جرائم الإرهاب الإلكتروني من منظور القانون الدولي، المرجع السابق، ص 38-37.

(64) انظر القانون اتحادي، رقم 7، دولة الإمارات العربية المتحدة، في شأن مكافحة الجرائم الإرهابية، لسنة 2014م، المادة 52،53،54، 62،63، وكذلك انظر مرسوم بقانون اتحادي، دولة الإمارات العربية المتحدة، بإصدار قانون الإجراءات الجزائية، رقم 38، لسنة 2022م، المادة 8، 42، 52، 67، 68، 73، 94، 113.

(65) انظر مرسوم بقانون اتحادي، رقم 34، دولة الإمارات العربية المتحدة، في شأن مكافحة الشائعات والجرائم الإلكترونية، لسنة 2021م، المادة 21، وجاء فيها "يعاقب بالسجن المؤبد والغرامة التي لا تقل عن (2,000,000) مليوني درهم ولا تزيد على (4,000,000)أربعة ملايين درهم، كل من أنشأ أو أدار موقعاً إلكترونياً أو أشرف عليه أو نشر معلومات أو بيانات على الشبكة المعلوماتية أو وسيلة تقنية معلومات، لجماعة إرهابية أو مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة بقصد تسهيل الاتصال بقياداتها أو أعضائها، أو لاستقطاب عضوية لها أو ترويج أو تحبيذ أفكارها أو تمويل أنشطتها، أو توفير المساعدة الفعلية لها، أو بقصد نشر أساليب تصنيع الاجهزة الحارقة أو الأسلحة أو الذخائر أو المتفجرات أو المواد الخطرة، أو أي أدوات أخرى تستخدم في الاعمال الإرهابية.

(66) انظر مرسوم بقانون اتحادي، رقم 38، دولة الإمارات العربية المتحدة، بإصدار قانون الإجراءات الجزائية، لسنة 2022م، المادة 383، 384، 385، 386.

(67) انظر مرسوم بقانون اتحادي، رقم 34، دولة الإمارات العربية المتحدة، في شأن مكافحة الشائعات والجرائم الإلكترونية، لسنة 2021م، المادة 24، وجاء فيها "يعاقب بالسجن المؤقت والغرامة التي لا تقل عن (200.000) مائتي ألف درهم ولا تزيد على (1.000.000) مليون درهم كل من أنشأ أو أدار موقعاً إلكترونياً أو أشرف عليه أو نشر معلومات أو برامج أو أفكار تتضمن إثارة للفتنة أو الكراهية أو العنصرية أو الطائفية إلكتروني أو الترويج أو التحبيذ لأي منها باستخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، إذا كان من شأنها الإضرار بالوحدة الوطنية أو السلم الاجتماعي أو الإخلال بالنظام العام أو الآداب العامة أو تعريض مصالح الدولة للخطر.

(68) انظر مرسوم بقانون اتحادي، رقم 34، دولة الإمارات العربية المتحدة، في شأن مكافحة الشائعات والجرائم الإلكترونية، لسنة 2021م، المادة 37، وجاء فيها "يعاقب بالحبس والغرامة التي لا تقل عن (250.000) مائتين وخمسين ألف درهم ولا تزيد على (1.000.000) مليون درهم، أو بإحدى هاتين العقوبتين، كل من ارتكب عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات أو على موقع إلكتروني، إحدى الجرائم الآتية: 1.الإساءة إلى أحد المقدسات أو الشعائر الإسلامية. 2 . الإساءة إلى أحد المقدسات أو الشعائر المقررة في الأديان الأخرى متى كانت هذه المقدسات والشعائر مصونة وفقاً لأحكام الشريعة الإسلامية.3. سب أحد الأديان السماوية المعترف بها .4 .تحسين المعاصي أو الحض عليها أو الترويج لها .فإذا تضمنت الجريمة إساءة للذات الإلهية أو لذات الرسل والأنبياء أو كانت مناهضة للدين الإسلامي أو جرحاً للأسس والمبادئ التي يقوم عليها، أو ناهض أو جرح ما علم من شعائر وأحكام الدين الإسلامي بالضرورة، أو نال من الدين الإسلامي، أو بشر بغيره أو دعا إلى مذهب أو فكرة تنطوي على شيء مما تقدم أو حبذ لذلك أو روج له، فيعاقب بالسجن المؤقت مدة لا تزيد على (7) سبع سنوات.

## المصادر

## References

**First: Legislation and constitutions:**

i. Federal Law No. 7, United Arab Emirates, on Combating Terrorist Crimes of 2014.
ii. Federal Decree-Law No. 34, United Arab Emirates, on Combating Rumours and Cybercrimes, for the year 2021.
iii. Federal Decree-Law No. 20, United Arab Emirates, on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organizations of 2018.
iv. Federal Decree-Law No. 55, United Arab Emirates, regarding the regulation of the media, for the year 2023.
v. Federal Decree-Law No. 45, United Arab Emirates, on the Protection of Personal Data for the year 2021.
vi. Federal Decree-Law No. 38, United Arab Emirates, promulgating the Code of Criminal Procedure of 2022.
vii. Decree of the President of the Arab Republic of Egypt, Law No. 94 of 2015, promulgating the Anti-Terrorism Law, available in the Official Gazette, Issue 33, August 15, 2015.
viii. The legal decision of the House of Representatives, Arab Republic of Egypt, by Law No. 175 of 2018, regarding combating information technology crimes, is present in the running.

**Second: Magazines:**

i. Al-Sir Al-Jilani Al-Amin Hammad and Muhammad Nasr Abdullah Nasr, The Concept of Electronic Terrorism and Ways to Combat It, Journal of Extremism and Armed Groups Issues, Volume 04, Issue 11, 2023.

ii. Engy Al-Mahdi, Electronic Terrorism: The Phenomenon and Repercussions of Use by Jihadist Organizations, National Social Journal, Volume Fifty-Eight, Issue One, January 2021.
iii. Hossam Fayez Abdel Hay, Electronic terrorism as a means of psychological warfare, a theoretical study, Journal of Research in the Fields of Specific Education, Issue Thirteen, 2017.
iv. Khaled Juma Sabit Ahmed Al-Makhmari, The Security Confrontation of Cyber Terrorism, Journal of Legal and Economic Research, Volume 58, Issue 2, October 2023.
v. Soleimani Mubarakeh, Electronic Terrorism and Ways to Combat It, Journal of Law and Political Science, No. 08, Vol. 01, 2017.
vi. Lalousofriadi bin Mujib, New Media in the Face of the Challenges of Electronic Terrorism, Al-Zahra, a semi-annual refereed magazine, seventeenth year, Issue 1, 2020.
vii. Lamia Mohamed Abdel Salam Judeh, The Role of the International Criminal Police Organization in Combating the Crime of International Terrorism, Journal of Jurisprudence and Legal Research, Forty-second Issue, 2023.
viii. Mohamed Khalifa Mohamed Suleiman Al-Hinai and Nizar Mohamed Ahmed, The Role of Artificial Intelligence in Combating the Crime of Financing Cyberterrorism, Perdana, International Journal of Academic Research, Social Sciences and Humanities, Volume 19, Issue 1, 2024.
ix. Mohamed Hamdi Abdel Alim Allam, Criminal Evidence in Electronic Terrorism Crimes, Journal of Extremism and Armed Groups Issues, Vol. 04, No. 11, 2023.
x. Muhammad Al-Tayeb Abdullah Khaled, Electronic Terrorism, Journal of the College of Sharia and Law, Volume 13, 2020.

xi. Mustafa Khalil Kamel Khalil, Cyberterrorism Crimes from the Perspective of International Law, Journal of the Faculty of Law, Volume V, Issue Two, December 2022.
xii. Nasser Al-Ali, International Efforts in Combating Cyberterrorism, Al-Researcher Journal for Academic Studies, Vol. 08, No. 01, Year 2021.

**Third: International Organizations:**

i. United Nations UNODC, New York, United Nations Office on Drugs and Crime, Vienna, The use of the Internet for terrorist purposes, June 2013.
ii. United Nations Office on Drugs and Crime, Study on Counter-Terrorism Legislation in the Arab Gulf States and Yemen, Vienna, 2009.

**Fourth**: **Websites**

i. The Official Portal of the UAE Government, Cyber Safety and Digital Security, available on the website, https://u.ae/ar-ae/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security/cyber-safety .
ii. Penetrating, available on the website, https://ar.m.wikipedia.org/wiki/%D9%85%D8%AE%D8%AA%D8%B1%D9%82 .
iii. Mahmoud Salameh, International and Regional Organizations in Combating Cyberterrorism, article in International Politics, January 2022, available on the official website of https://www.researchgate.net/publication/357578485 .
iv. Features of the global transition to the "post-information" phase, available on the website, https://futureuae.com/ar/Mainpage/ltem/4267.

v. Hisham Bashir, Opinions on the Gulf, Electronic Terrorism in the Light of the Information Revolution, Issue 92, May 2012, available on the website https://mail.araa.sa/index.php?option=com_conten&view=article&id=244:2014-06-13-16-21-31&catid=132&Itemid=294 .